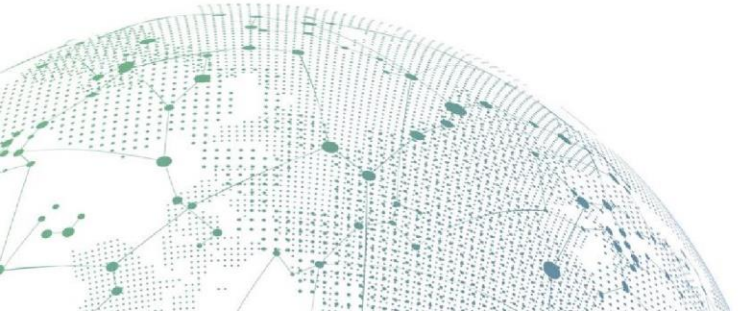
SANGFOR

Sangfor Metode Pemrosesan Peristiwa Keamanan



Daftar Isi

Berdasarkan dari pengalaman respon keadaan darurat, umpan balik fenomena langsung biasanya dibagi menjadi dalam tiga tipe:

1. Webpage di hack, seperti melalui perangkat, unit pengatur atau customer menemukan sendiri bahwa telah diberikan link gelap (konten web seperti pornografi, obat-obatan atau perjudian), atau tergantung webshell, tipe ini adalah masalah web-based.
2. Anomali visual dari host itu sendiri seperti blue screen (bisa jadi oleh ransomware atau mungkin masalah non-security seperti masalah driver), berkas-berkas terenkripsi (ransomware), server gagal terkoneksi (Bisa jadi mining atau program yang dikecualikan).
3. Anomali lalu lintas menengah, seperti laporan perangkat sekuriti C&C komunikasi (bisa jadi program yang berbahaya), lalu lintas internal DOS (bisa jadi program berbahaya), jaringan luar DOS, perangat sekuriti menemukan kerentanan (notifikasi kerentanan) dan lainnya.

Kasus kasus diatas mencakup sebagian besar fenomena, beberapa kasus dapat digabungkan dengan beberapa skenario diatas. Berdasarkan dari analisa situasi aktual, ada beberapa adegan yang tidak terlalu terlihat dan bisa jadi hanya bagian dari botnet logs. Apapun bentuknya, pengguna perlu untuk memeriksa beberapa langkah sebelum meningkatkan masalahnya. Pengguna bisa mengekskalasi masalah ke kantor pusat.

1 Masalah Keamanan Web-base

1.1 Fenomena:

NGAF home page atau key page telah dirusak, bermacam-macam informasi buruk akan muncul, atau website telah diarahkan ke situs berbahaya.

1.2 Penyelesaian Masalah:

1. Cari nama domain dan katakunci oleh alat pencarian, contoh: situs: sangfor.com dan lainnya. Cek pada halaman untuk melihat apakah diloncatkan ke tautan halaman hitam.
2. Gunakan alat EDR untuk memeriksa server yang abnormal untuk melihat apakah ada program yang berbahaya dan export hasil pemberhentian.

1.3 Pengumpulan Informasi sebelum umpan balik:

1. Ketidaknormalan Waktu: konsultasi dengan admin web, perkiraan waktu saat website dirusak, seperti waktu ketika administrator menemukan bahwa situs web telah dirusak sekitar 18/09/2018 1500pm.
2. Karakteritas Host tidaknormal: situs web telah di hijack, akses melalui search engine, dan ter-hijack ke situs perjudian (dilaporkan oleh otoritas peraturan untuk memberikan dokumen notifikasi yang relevan)
3. Informasi dan cakupan host yang terpengaruh: seperti windows server dengan BB yang terpasang telah dirusak.
4. Jam kerja pengguna dan status akun: jika klien biasanya mengunjungi situs web dari jam 0900 sampai 1730, ketika selesai bekerja seharusnya tidak dapat login.
5. Konfigurasi Security device policy: ada NGAF, aktifkan WAF dan ISP proteksi NGAF, perangkat lunak anti-virus terpasang pada server, dan metode login perangkat keamanan terkait perlu disediakan.
6. Status log audit: Konsultasi dengan administrasi web tentang situs web apakah diaktifkan log web akses.
7. Sediakan laporan pemeriksaan EDR (Laporan EDR dalam format HTML).
8. Masukkan toolkit pemecahan masalah darurat aplikasi umum ke dalam server yang perlu untuk pemecahan masalah.

1.4 Catatan:

jika langkah-langkah diatas tidak dapat membenarkan masalah selanjutnya berikan sesi remote (jika customer langsung mengajukan informasi ke kantor pusat, mereka mempunya hak untuk menolak untuk mengajukan remote. Semua layana keamanan perlu jarak jauh, ini tidak akan dijelaskan nanti).

2 Ransomware

2.1 Fenomena:

Berkas-berkas pada server atau PC terenkripsi dan muncul informasi pemerasan.

2.2 Pemecahan masalah:

1. Periksa akhiran dari berkas yang terenkirpsi di host.
2. Gunakan **segalanya** untuk mencari nama akhiran yang berhubungan dengan ransomware dan temukan berkas dengan waktu modifikasi paling awal.
3. Gunakan alat EDR botnet untuk memeriksa server abnormal dan jalankan alat deteksi NSA untuk melihat jika MS17-010 vulnerability patch.
4. **eventvwr** periksa log keamanan untuk melihat telah terhapus.

2.3 Kumpulkan informasi sebelum umpan balik:

1. Ketidaknormalan waktu: Waktu ketika berkas terenkripsi.
2. Ketidaknormalan karakteritas Host: akhiran berkas enkripsi.
3. Informasi dan cakupan host yang terpengaruh: seperti 1 windows server telah terenkripsi.
4. Aturan alat keamanan dan konfigurasi: ada NGAF, WAF dan ISP proteksi NGAF telah diaktifkan, perangkat lunat anti-virus telah diapasang pada server, dan metode login perangkat keamanan terkait perlu disediakan.
5. Status log audit: Konsultasi dengan administrasi web tentang situs web apakah diaktifkan log web akses.
6. Menyediakan laporan pemeriksaan EDR botnet dan periksa MS17-010 vulnerability patch telah terpasang atau tidak.
7. Masukkan toolkit pemecahan masalah darurat aplikasi umum ke dalam server yang perlu untuk pemecahan masalah.

3 Ransomware variant

3.1 Fenomena:

Blue screen muncul pada banyak server.

3.2 Pemecahan Masalah:

1. Jalankan alat deteksi NSA untuk memeriksa MS17-010 vulnerability patch apakah sudah diinstall atau belum.
2. Periksa task manager, apakah ada proses msecvc2.0 atau tidak.
3. Periksa jika ada berkas C:\Windows\qeriuwjhrf.
4. Gunakan alat DER botnet untuk memeriksa server tidaknormal.

3.3 Kumpulkan informasi sebelum umpan balik:

1. Ketidaknormalan waktu: waktu server ketika blue screen
2. Ketidaknormalan karakteritas Host: blue screen muncul pada server.
3. Informasi dan cakupan host yang terpengaruh: seperti 2 window server telah blue screen.
4. Aturan alat keamanan dan konfigurasi: ada NGAF, WAF dan ISP proteksi NGAF telah diaktifkan, perangkat lunat anti-virus telah diapasang pada server, dan metode login perangkat keamanan terkait perlu disediakan.
5. Menyediakan laporan pemeriksaan EDR botnet dan periksa MS17-010 vulnerability patch telah terpasang atau tidak.
6. Masukkan toolkit pemecahan masalah darurat aplikasi umum ke dalam server yang perlu untuk pemecahan masalah.

4 Mining virus

4.1 Fenomena:

Status CPU server tinggi, ketidaknormalan proses yang menempati CPU untuk waktu yang lama, dan NGAF botnet mendeteksi ketidaknormalan komunikasi.

4.2 Pemechan Masalah:

1. Gunakan alat DER botnet untuk memeriksa server.

2. Gunakan hacker proses untuk menemukan proses yang mencurigakan dan kelakukan koneksi jaringan mereka berdasarkan peringkat penggunaa CPU.
3. Pada Virustotal tay ThreatBook, periksa nama domain atau alamat IP dari koneksi yang berhasil apakah mempunyai karakteristik kumpulan tambang.

4.3 Kumpulkan informasi sebelum umpan balik:

1. Ketidaknormalan waktu: Waktu saat administrasi menemukan masalah pada server.
2. Ketidaknormalan karakteritas Host: CPU Server tidak normal.
3. Informasi dan cakupan host yang terpengaruh: Seperti 1 server tidak normal.
4. Aturan alat keamanan dan konfigurasi: ada NGAF, WAF dan ISP proteksi NGAF telah diaktifkan, perangkat lunat anti-virus telah diapasang pada server, dan metode login perangkat keamanan terkait perlu disediakan.
5. Sediakan laporan pemeriksaan EDR botnet.
6. Masukkan toolkit pemecahan masalah darurat aplikasi umum ke dalam server yang perlu untuk pemecahan masalah.

4.4 Catatan:

Ketika masalah mining ditingkatkan ke departemen layanan keamaan, virus harus dalama keadatan periode aktif. Jika adalah lalu lintak tidak normal, maka dapat ditingkatkan. Jika tidak ada lalu lintas yang tidak normal, maka ini direkomendasikan customer untuk memonitoring terlebih dahulu dan hapus ketika terjadi lalu lintas.

5 Program Berbahaya

5.1 Fenomena:

1. Fenomena1: Host 3389 remote desktop akan tiba-tiba putus ketika digunakan, keluar ke tampilan Windows login dan login kembali akan muncul pemberitahuan remote desktop sedang sibuk.
2. Fenomena2: Ditemukan bahwa host mempunyai kelakukan komunikasi yang tidak normal pada NGAF bonet.
3. Fenomena3: Server mempunyai ketidaknormalan seperti menyangkut, penggunaan memory yang tinggi, web browsing yang lambat dan konektivitas jarngan yang tidak dapat dilepaskan.

5.2 Pemecahan Masalah:

1. Periksa alat keamanan yang terhubung apakah adalah hubungan komunikasi yang tidak normal.
2. Gunakan Wireshark atau Colasoft untuk mendapatkan paket, ambil lalu lintas tidak normal.
3. Gunakan alat EDR botnet untuk memeriksa server yang tidak normal.

5.3 Kumpulkan informasi sebelum umpan balik:

1. Ketidaknormalan waktu: Waktu ketika admnistrasi menemukan masalah pada server.
2. Ketidaknormalan karakteritas Host: CPU server tidak normal, penggunaan memori yang tinggi, NGAF menemukan botnet.
3. Informasi dan cakupan host yang terpengaruh: Seperti 2 Windows server mempunyai masalah.
4. Aturan alat keamanan dan konfigurasi: ada NGAF, WAF, ISP, dan APT proteksi NGAF, telah diaktifkan, konfiurasi adalah normal , perangkat lunat anti-virus telah diapasang pada server, dan metode login perangkat keamanan terkait perlu disediakan.
5. Sediakan laporan pemeriksaan EDR botnet.
6. Masukkan toolkit pemecahan masalah darurat aplikasi umum ke dalam server yang perlu untuk pemecahan masalah.

5.4 Catatan:

1. Ketika ada masalah lalulintas perlu diteruskan ke departemen layanan keamanan, ketidaknormalan host harus dalam keadaan periode aktif. Jika ada ketidaknormalan lalulintas maka dapat dilanjutkan. Jika tidka ada ketidaknormalan lalulintas, direkomendasikan bahwa kustomer lebih dahulu memantau dan hapus lalulinta yang ada.
2. Jika ketika proses pemecahan masalah ditemukan bukan fenomena 3 bukan masalah keamana, dibutuhkan penyelesaian oleh kustomer lokasi petugas pemeliharaan.

6 Internal abnormal traffic

6.1 Fenomena:

Alat keamanan seperti NGAF menemukan ketidaknormalan lalulintas internet, seperti traffic spikes, host akses ke domain name berbahaya, serangan APR intranet, serangan flood intranet,

pemindaian port intranet, jaringan mulai banayak menginisiasi pemindaian host-to-public dan lainnya.

6.2 Pemecahan Masalah:

1. Periksa NGAF untuk menemukan host yang bermasalah untuk ketidaknormalan lalulintas yang keluar.
2. Gunakan alat EDR botnet untuk mengecek server yang tidak normal.
3. Gunakan proses peretas untuk memeriksa proses yang mencurigakan dan perilaku network mereka.

6.3 Kumpulkan informasi sebelum umpan balik:

1. Ketidaknormalan waktu: Waktu ketika admnistrasi menemukan masalah pada server.
2. Ketidaknormalan karakteritas Host: Seperti jika alamat (nama domain) dikases oeh host adalah ditandai berbahaya oleh Virustotal atau host diinisiasi dengan jumlah pemindaian yang banyak pada port publik.
3. Informasi dan cakupan host yang terpengaruh: Seperti 1 server windows, 1 PC windows 7 mempunyai masalah.
4. Aturan alat keamanan dan konfigurasi: ada NGAF, WAF, ISP, dan APT proteksi NGAF, telah diaktifkan, konfiurasi adalah normal , Tencent Manager Anti-virus telah diapasang pada server, dan metode login perangkat keamanan terkait perlu disediakan.
5. Sediakan laporan pemeriksaan EDR botnet.
6. Sediakan paket lalulintas tidak normal host.
7. Masukkan toolkit pemecahan masalah darurat aplikasi umum ke dalam server yang perlu untuk pemecahan masalah.

6.4 Catatan:

1. Ketika ada masalah lalulintas perlu diteruskan ke departemen layanan keamanan, ketidaknormalan host harus dalam keadaan periode aktif. Jika ada ketidaknormalan lalulintas maka dapat dilanjutkan. Jika tidka ada ketidaknormalan lalulintas, direkomendasikan bahwa kustomer lebih dahulu memantau dan hapus lalulinta yang ada.
2. Kejadian Lalulintas tidak normal dapat mempengaruhi unduh P2P atau pengguna menggunakan agent perangkat lunak. Jika masalah ketidakamanan ditemukan saat pemecahan masalah, dibutuhkan penyelesaian oleh kustomer lokasi petugas pemeliharaan.

7 Internal DOS

7.1 Fenomena:

Alat keamanan seperti NGAF menemukan hots pada jaringa internal mengirimkan banyak sekali lalulntas, menyebabkan pengguna jaringan gagal dan alat jaringan dan host down.

7.2 Pemecahan Masalah:

1. Login ke NGAF dan temukan host yang mengirimkan banyak sekali paket yang tidak normal.
2. Gunakan Wireshark atau Colasoft untuk mendapatkan lalulintas dan analisa tidak normal.
3. Gunakan alat EDR botnet untuk memeriksa server yang tidak normal.

7.3 Kumpulkan informasi sebelum umpan balik:

1. Ketidaknormalan waktu: Waktu ketika admnistrasi menemukan masalah pada server.
2. Ketidaknormalan karakteritas Host: Jika host yang dimaksud memindai banyak sekali host dalam intranet kemudian host yang lain pada intranet akan down.
3. Informasi dan cakupan host yang terpengaruh: Seperti 1 server window, 3 PC windows 7 tidak normal.
4. Aturan alat keamanan dan konfigurasi: ada NGAF, WAF, ISP, dan APT proteksi NGAF, telah diaktifkan, konfiurasi adalah normal , Tencent Manager Anti-virus telah diapasang pada server, dan metode login perangkat keamanan terkait perlu disediakan.
5. Sediakan laporan pemeriksaan EDR botnet.
6. Sediakan paket lalulintas tidak normal host.
7. Masukkan toolkit pemecahan masalah darurat aplikasi umum ke dalam server yang perlu untuk pemecahan masalah.

8 Pemberitahuan Kerentanan

8.1 Fenomena:

Klien diberitahu oleh otoritas pengatur superior bahwa ada tautan hitam, websheel pada situs web dan ada lalulintas yang tidak normal pada keluaran jaringan.

8.2 Pemecahan Masalah:

1. Jika notifikasi tentang tatutan hitam atau peristiwa webshell, FAE akan membutuhkan pemeriksaan apakah ada false positive berdasarkan dari konten yang diberikan oleh laporan dan gunakan alat Sangfor Webshell untuk memeriksa berkas-berkas yang dimiliki server.

2. Jika pemberitahuan adalah lalulintas tidak normal, FAE akan membutuhkan alat EDR botnet untuk memeriksa berdsarkan dari konten laporan.

8.3 Kumpulkan informasi sebelum umpan balik:

1. Sediakan dokumen pemberitahuan oleh otoritas pengatur superior, langsung mendapatkannya.
2. Sediakan investigasi apa dan kesimpulan yang telah dilakukan hanya masalah yang tidak dapat ditentukan setelah penyaringan FAE diterima.
3. Sediakan metode jarak jauh untuk server yang tidak normal.
4. Masukkan toolkit pemecahan masalah darurat aplikasi umum ke dalam server yang perlu untuk pemecahan masalah.

8.4 Catatan:

Jika konten dari notifikasi hanya untuk serangan external dari jaringan publik server klien dan tidak ada bukti bahwa serangan itu berhasil, keamanan penghalang tidak akan memberhentikannya karena server akan dijadikan subjek ketika server di buka ke jaringan public. Untuk masalah tersebut, FAE akan perlu menjelaskan ke kustomer.

9 Masalah Keamana Lain

9.1 Fenomena:

Masalah dan fenomena ketidaknormalan yang tidak termasuk cakupan deskripsi diatas.

9.2 Pemecahan Masalah:

1. Gunakan alat EDR botnet untuk memeriksa server yang tidak normal.

9.3 Kumpulkan informasi sebelum umpan balik:

1. Ketidaknormalan waktu: Waktu ketika admnistrasi menemukan masalah pada server.
2. Ketidaknormalan karakteritas Host: Jika host yang dimaksud memindai banyak sekali host dalam intranet kemudian host yang lain pada intranet akan down.

3. Informasi dan cakupan host yang terpengaruh: Seperti 1 server window, 3 PC windows 7 tidak normal.
4. Security device policy and configuration: There is a NGAF, NGAF is enabled WAF, IPS and APR protection, configuration is normal, Tencent Manager Anti-virus is installed on the PC, and login method of related security device need to provide.
5. Sediakan laporan pemeriksaan EDR botnet.
6. Sediakan paket lalulintas tidak normal host.
7. Investigasi dan kesimpulan yang telah dibuat: Proses telah selesai, koneksi jaringan dan tidak ada hal yang tidak normal ditemukan.
8. Masukkan toolkit pemecahan masalah darurat aplikasi umum ke dalam server yang perlu untuk pemecahan masalah.

Tautan unduhan untuk alat terkait

1. Sangfor AntiBot: http://go.sangfor.com/edr-tool-20180824
2. Colasoft : https://www.colasoft.com/capsa-free/
3. Toolkit pemecahan masalah darurat aplikasi umum:

   https://drive.google.com/open?id=1H-LiJypMvSO2HTjdfjC9bjMOK1ZccYjg

SANGFOR