"INGATLAH BAHWA : KECHILAFAN SATU ORANG SAHAJA TJUKUP SUDAH MENJEBABKAN KERUNTUHAN NEGARA" (ROEBIONO KERTOPATI)

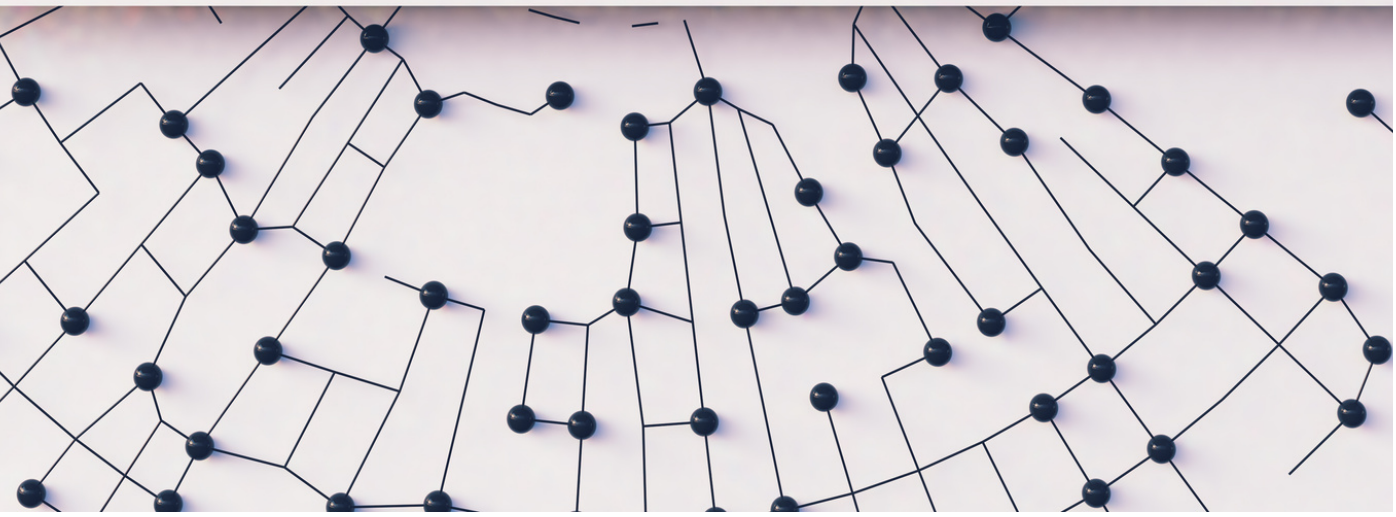
Panduan Keamanan

Mylobot

malware

Juni 2022

TLP: WHITE

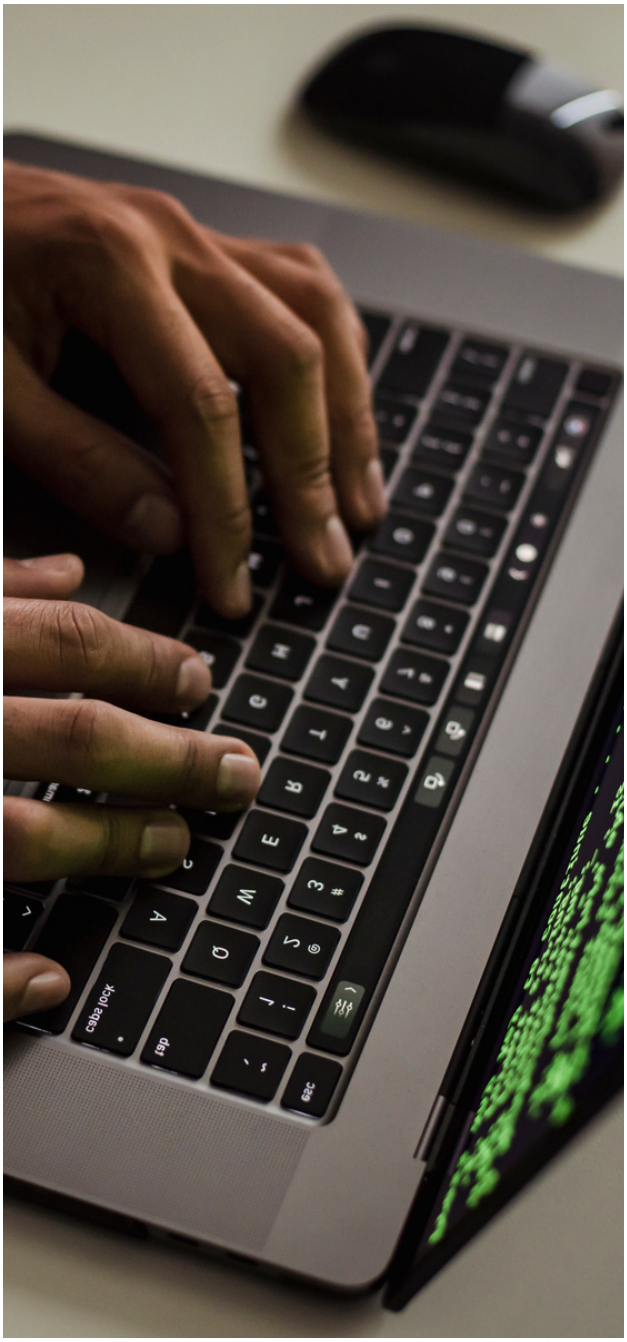


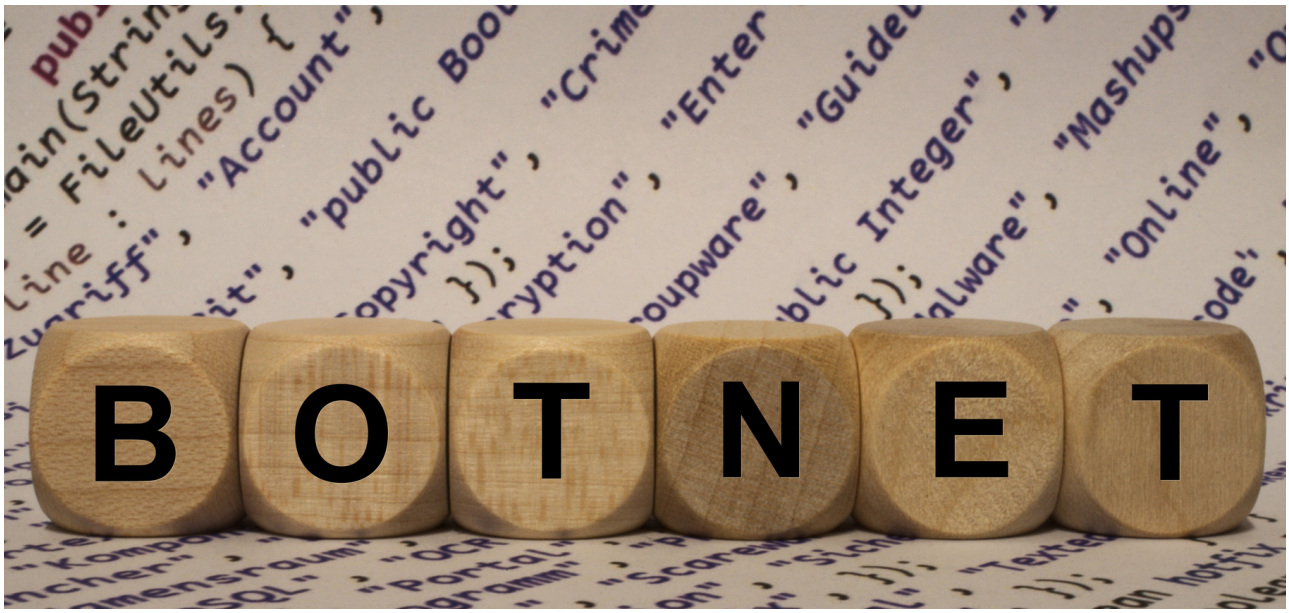
Id-SIRTII/CC – BSSN
Jalan Harsono RM No. 70 Ragunan
Jakarta Selatan, 12550, Indonesia

Ditandatangani secara elektronik oleh:
Koordinator Kelompok/Fungsi Operasi Deteksi, Penanggulangan dan Pemulihan, Penanganan Insiden dan Krisis Siber Nasional

Taufik Arianto, S.ST., M.Kom.
Pembina (IV/a)

Daftar Isi





BOTNET

Botnet adalah jaringan komputer yang terinfeksi dimana jaringan tersebut dikendalikan secara jarak jauh (*remote*) oleh pelaku kejahatan siber (*cybercriminal*). Istilah botnet berasal dari gabungan "*robot*" dan "*network*". Bot berfungsi sebagai alat otomatisasi serangan massal, seperti pencurian data, keruskaan server, dan distribusi *malware*.

Komputer yang telah terinfeksi botnet akan dimanfaatkan oleh cybercriminal untuk menipu orang/pihak lain, atau menyebabkan gangguan tanpa seizin pemilik perangkat. Selain itu, dampak lain yang dirasakan oleh pemilik perangkat yang terinfeksi dapat berupa meningkatnya tagihan listrik, peforma komputer menjadi lebih lambat dan tidak stabil, dan pencurian data pribadi.

Salah satu jenis botnet yang sedang banyak dibicarakan adalah MyloBot Botnet. MyloBot merupakan varian Botnet yang menyerang sistem operasi Windows dan berpotensi merubah pengaturan-pengaturan perangkat yang terinfeksi.

730.946.448

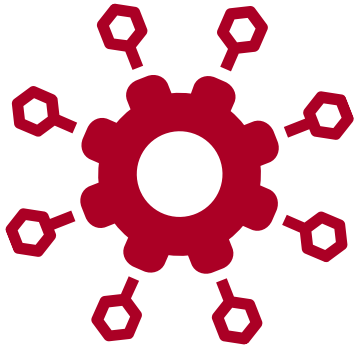
Menurut Laporan Tahunan Monitoring Keamanan Siber Tahun 2021 BSSN, MyloBot masuk ke dalam **Top 10 *Malware*** dengan jumlah anomali tertinggi. Jumlah anomali MyloBot yaitu sebanyak **730.946.448 anomali**.

MYLOBOT BOTNET

MyloBot Botnet menargetkan sistem operasi Microsoft Windows yang menyebar melalui spam *email* dan unduhan *file* yang telah terinfeksi. Setelah terinstal, botnet mematikan *Windows Defender* dan *Windows Update* sembari memblokir *port* tambahan di Firewall. Selain itu, botnet juga mematikan dan menghapus *file* .exe yang berjalan dari folder %APPDATA%, yang dapat menyebabkan hilangnya data.

MyloBot Botnet adalah salah satu jenis botnet yang memiliki kemampuan mengunduh dan mengeksekusi semua jenis muatan setelah berhasil menginfeksi. Dengan kata lain, fungsi utama botnet memungkinkan penyerang untuk mengambil kendali penuh atas sistem pengguna, salah satunya berfungsi sebagai gerbang untuk mengunduh muatan tambahan dari server *Command and Control*. Perilaku umum Mylobot berupa panggilan balik (*callback*) ke domain-domain yang dihasilkan dari *Domain Generation Algorithm* (DGA). DGA ini mencakup teknik pemilihan huruf atau angka secara acak untuk membentuk domain.

Mylobot Botnet juga memiliki teknik *anti-VM* dan *anti-sandboxing* yang canggih untuk menghindari deteksi dari proses analisis. Misal, MyloBot Botnet akan menunggu sampai 14 hari sebelum melakukan interaksi dengan server Command and Control dari penyerang. Teknik penundaan ini digunakan untuk menghindari deteksi dari *sandbox environment*.

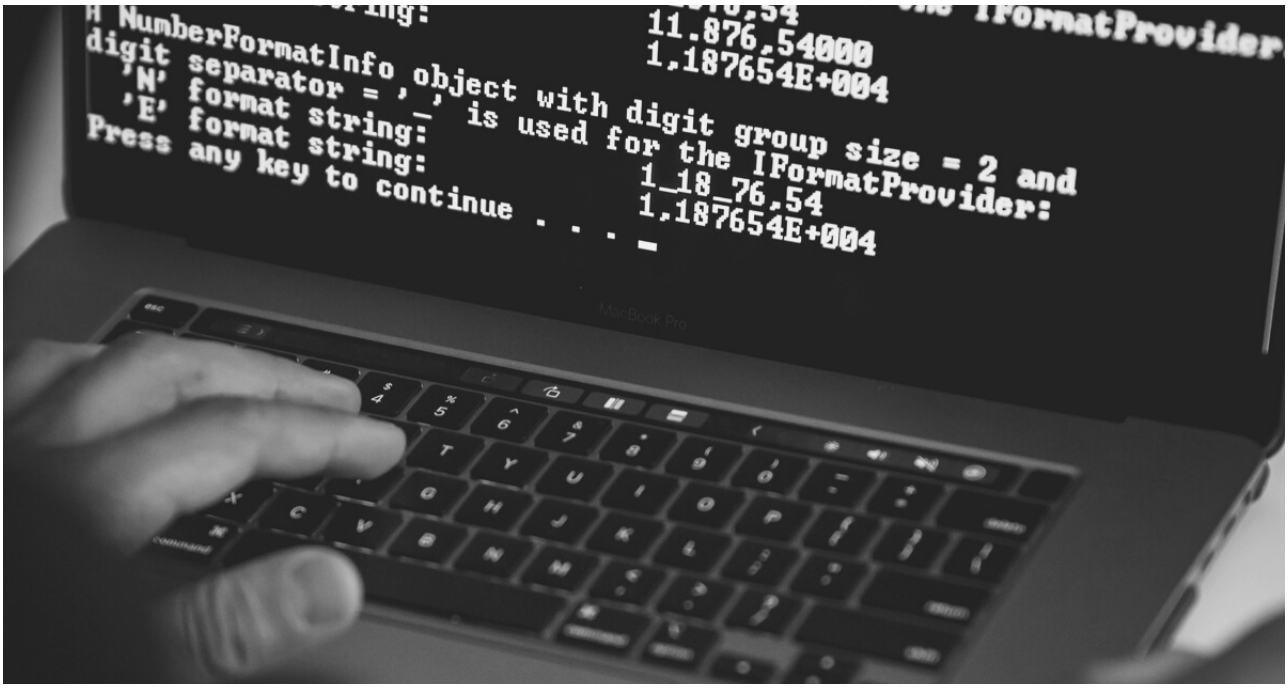


KAPABILITAS MYLOBOT

MyloBot botnet pertama kali terdeteksi pada tahun 2018 dan merupakan salah satu Botnet yang cukup populer menginfeksi secara global pada saat ini. MyloBot botnet memiliki sejumlah kemampuan, diantaranya:

- Teknik *Anti-VM;*
- Teknik *Anti-Sandboxing;*
- Teknik *Anti-Debugging;*
- Membungkus bagian internal dari *malware* ini dengan enkripsi;
- *Code Injection*;
- *Process Hollowing* - teknik dimana penyerang membuat proses baru dalam status "*suspended*", dan menggantikan kode proses tersebut dengan kode berbahaya bertujuan agar tetap tidak terdeteksi;
- Reflektif EXE - mengeksekusi *file* EXE secara langsung dari memori, tanpa meninggalkan artefak di dalam *disk* penyimpanan; dan
- Mekanisme *delay* 14 hari sebelum melakukan akses ke server *Command and Control* (C2).

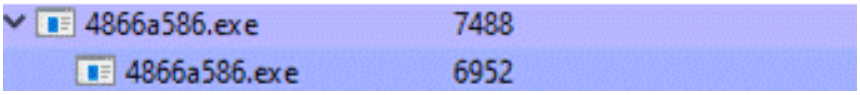
Pada MyloBot botnet versi 2022 secara umum tidak banyak perbedaan yang ditemukan berkaitan dengan *malware* ini. Beberapa teknik *Anti-Debugging* dan *Anti-VM* dihilangkan, dengan *malware* varian 2022 ini lebih banyak menggunakan teknik injeksi, kemudian *payload* tahap kedua yang diunduh dari C2 server digunakan untuk mengirimkan pesan *email* berupa ancaman/pemerasan.



RANTAI INFEKSI MYLOBOT

STAGE 1

Pada tahap ini malware menjalankan sejumlah teknik *anti-debugging* untuk menghindari analisis melalui teknik debugging yang umum dilakukan oleh periset *malware*. Kemudian teknik lain yang digunakan adalah *malware* melakukan penundaan proses dengan periode waktu tertentu, apabila proses tersebut telah berakhir baru *malware* tersebut aktif dengan memanggil proses tertentu. Pada tahap ini *malware* ini menjalankan teknik "*Process Hollowing*", dimana *malware* membuat proses baru dimana memori dari program eksekusi yang dimuat digantikan dengan resource dari *file* yang telah didekode sebelumnya.



Teknik *Hollowed Process*

STAGE 2

Pada tahap ini malware tetap menjalankan teknik *Anti-VM Checking*, dengan melakukan pencarian informasi pada sistem yang menjalankan dengan melakukan pegecekan informasi *strings* VMWARE, VBOX, VIRTUAL HD dan QEMU. Selanjutnya, *malware* ini juga melakukan pengcekan *persistent software* atau *malware* lainnya yang melakukan *persistent* pada komputer yang terinfeksi, dengan melakukan pencarian informasi berikut pada komputer yang terinfeksi:

- `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce`
- `HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce`
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`

Hal ini bertujuan untuk melakukan penghapusan *malware* yang telah ada atau menginfeksi komputer korban sebelumnya. Pada tahap ini *malware* juga membuat folder baru pada direktori **C:\ProgramData**. *Malware* ini mencari program svchost.exe pada direktori sistem dan menjalankannya dalam mode "*suspended*". Setelah itu dengan menggunakan teknik *APC Injection*, *malware* ini menginjeksi dirinya sendiri pada proses "svchost.exe"

STAGE 3

Pada tahap ini *malware* bertugas untuk membuat persistensi. Pertama *malware* ini menuliskan *file* executable yang dijalankan pada tahap 1 ke dalam folder yang telah dibuat, kemudian membuat nilai *registry key* baru dalam *path*.

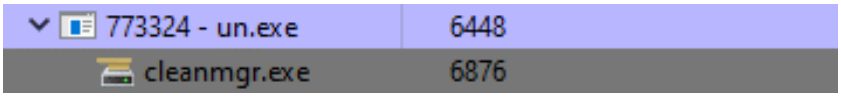
Teknik Persistensi

STAGE 4

Pada tahapan ini *malware* melakukan kontak ke C2 Server untuk mengunduh *file* berbahaya pada tahap berikutnya.

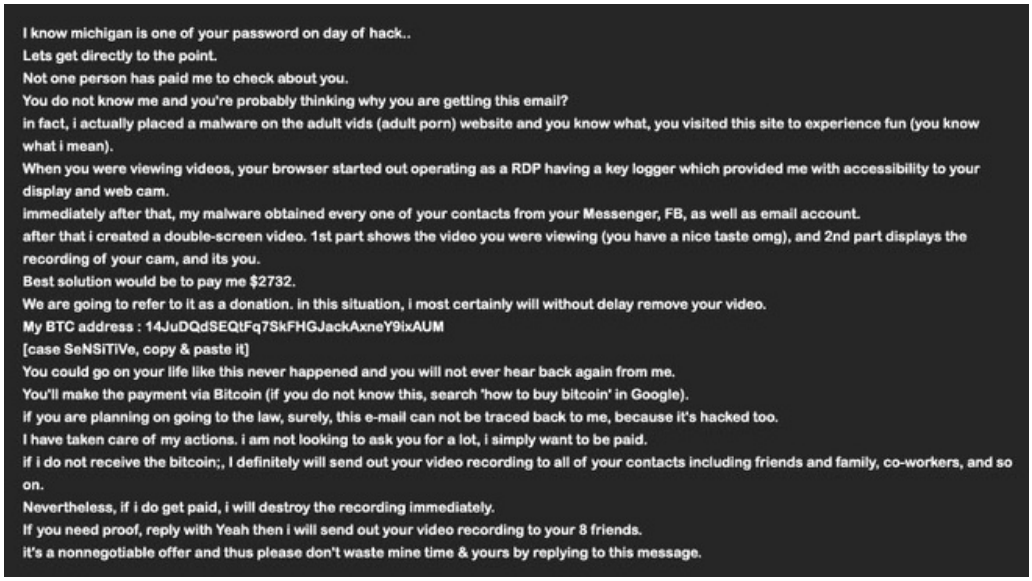
STAGE 5

Pada tahap ini *malware* menjalankan teknik injeksi seperti pada tahap 1, yakni dengan menggunakan teknik ***Hollowed Process***, namun *resource* yang dimuat berbeda dengan tahapan sebelumnya. Setelah itu *malware* menjalankan proses "cleanmgr.xe" jika ada, namun jika tidak maka *malware* menjalankan "svchost.exe".



Injeksi Proses "cleanmgr.exe"

MyloBot juga didesain untuk memanfaatkan komputer yang terinfeksi untuk mengirimkan pesan ancaman kepada penerima, yang mengintimidasi penerima pesan mengenai perilaku penerima pesan *email* yang memiliki kebiasaan mengunjungi situs porno dan mengancam akan menyebarkan video yang diduga direkam dengan membobol komputer korban.


I know michigan is one of your password on day of hack..
Lets get directly to the point.
Not one person has paid me to check about you.
You do not know me and you're probably thinking why you are getting this email?
in fact, i actually placed a malware on the adult vids (adult porn) website and you know what, you visited this site to experience fun (you know what i mean).
When you were viewing videos, your browser started out operating as a RDP having a key logger which provided me with accessibility to your display and web cam.
immediately after that, my malware obtained every one of your contacts from your Messenger, FB, as well as email account.
after that i created a double-screen video. 1st part shows the video you were viewing (you have a nice taste omg), and 2nd part displays the recording of your cam, and its you.
Best solution would be to pay me $2732.
We are going to refer to it as a donation. in this situation, i most certainly will without delay remove your video.
My BTC address : 14JuDQdSEQtFq7SkFHGJackAxneY9ixAUM
[case SeNSiTiVe, copy & paste it]
You could go on your life like this never happened and you will not ever hear back again from me.
You'll make the payment via Bitcoin (if you do not know this, search 'how to buy bitcoin' in Google).
if you are planning on going to the law, surely, this e-mail can not be traced back to me, because it's hacked too.
I have taken care of my actions. i am not looking to ask you for a lot, i simply want to be paid.
if i do not receive the bitcoin;, I definitely will send out your video recording to all of your contacts including friends and family, co-workers, and so on.
Nevertheless, if i do get paid, i will destroy the recording immediately.
If you need proof, reply with Yeah then i will send out your video recording to your 8 friends.
it's a nonnegotiable offer and thus please don't waste mine time & yours by replying to this message.

Contoh *email* ancaman

Pada umumnya, setelah terinfeksi oleh botnet, komputer menjadi bagian dari botnet – jaringan komputer yang terinfeksi atau zombie yang dikendalikan dari jarak jauh oleh pelaku ancaman atau *threat actor*. Jadi tidak hanya komputer Anda yang terinfeksi dan keamanan internet Anda yang terganggu, tetapi sumber daya sistem Anda dan *bandwidth* Anda digunakan oleh pelaku untuk membantu mereka menyerang pengguna lain yang tidak curiga atau bahkan bisnis lain. Potensi kejahatan dunia maya yang sangat besar ini menjadikan botnet yang oleh beberapa pakar keamanan diyakini sebagai ancaman paling berbahaya di internet saat ini.

Botnet tersebut terdiri dari ratusan atau ribuan perangkat yang terinfeksi memiliki sumber daya yang diperlukan untuk melakukan tindakan jahat skala tinggi seperti:

- Pengiriman spam massal yang membanjiri jutaan kotak masuk dalam hitungan detik;
- Serangan DoS dan DDoS yang merusak seluruh situs web dan dapat menempatkan bisnis yang sah dalam masalah serius;
- Serangan peretasan paksa dengan memecahkan kata sandi dan tindakan keamanan internet lainnya;
- Pencurian identitas dan penipuan internet dengan mengumpulkan informasi pribadi dari pengguna yang terinfeksi.

Dampak MyloBot jika berhasil menginfeksi komputer Anda, antara lain:

- Memungkinkan pelaku untuk menginstal beberapa jenis *malware* lainnya di perangkat Anda. Hal ini dilakukan oleh pelaku untuk mendukung aksinya. Malware yang diinstal seperti trojan perbankan, *keylogger*, dan *malware* lainnya.
- Pelaku kejahatan juga mungkin melakukan monitor aktivitas apa saja yang dilakukan oleh Anda.
- Monitoring yang dilakukan pelaku serta akses terhadap perangkat korban memungkinkan mereka mendapatkan informasi pribadi yang tersimpan pada perangkat, atau pun informasi yang dimasukkan tanpa sepengetahuan dari korban.
- Modifikasi *file* memungkinkan dilakukan oleh pelaku. Pelaku juga dapat menambahkan *file malicious* pada perangkat Anda untuk melakukan kejahatan lainnya.

INDICATOR OF COMPROMISE

NILAI HASH

SHA256 -
6fcd36052b242bc33e90577e9a9cf5dc91bc7c5f3ad587b0d45ab4a7cb7b73b3
SHA1 -
35b4faaa4a98fa141d1388ac9b0adba0ac0d4a3d

CVE

CVE-2017-11882

PATH

HKCU\Software\Microsoft\Windows\CurrentVersion\Run
C:\ProgramData\{Random String}\{nama random file}.exe

BITCOIN ADDRESS

14JuDQdSEQtFq7SkFHGJackAxneY9ixAUM

COMMAND AND CONTROL SERVER

- 46[.]166[.]173[.]180
- 74[.]222[.]19[.]63
- 70[.]36[.]107[.]38
- 74[.]222[.]19[.]103
- 70[.]36[.]107[.]39
- 217[.]23[.]13[.]62
- 89[.]38[.]98[.]48
- 212[.]8.242[.]104
- 217[.]23[.]3[.]15
- 109[.]236[.]85[.]150
- 70[.]36[.]107[.]154
- 75[.]126[.]102[.]251
- 109[.]236[.]87[.]49
- 89[.]38[.]98[.]165
- 109[.]236[.]85[.]21
- 109[.]236[.]85[.]154
- 89[.]39[.]107[.]19
- 89[.]39[.]105[.]82
- 109[.]236[.]85[.]147
- 109[.]236[.]85[.]93
- 217[.]23[.]6[.]62
- 109[.]236[.]85[.]135
- 109[.]236[.]85[.]153

IOC LAINNYA

https://github.com/IdSIRTII/MyloBot

Terdapat beberapa rekomendasi yang dapat dilakukan untuk mencegah kerentanan tersebut. Jika anda adalah Administrator jaringan yang berperan dalam mengelola dan menjaga jaringan, Anda disarankan untuk melakukan langkah-langkah sebagai berikut:

- Mewajibkan semua akun dengan *login* sandi yang kuat dan unik (misalnya, akun layanan, akun admin, dan akun admin domain). Sandi yang digunakan sangat disarankan untuk tidak digunakan kembali di banyak akun atau disimpan di sistem;

- Menerapkan autentikasi multi-faktor (*Multi-Factor Authentication*/MFA) untuk semua layanan jarak jauh (*remote*), terutama untuk *email* web, VPN (*Virtual Private Network*), dan akun yang mengakses sistem penting;

- Melakukan pembaruan semua sistem operasi dan perangkat lunak secara rutin. Hal yang perlu diprioritaskan adalah untuk menambal kerentanan yang diketahui/dieksploitasi;

- Menghapus akses yang tidak perlu ke pembagian administratif, terutama ADMIN$ dan C$. Jika ADMIN$ dan C$ dianggap perlu secara operasional, lakukan pembatasan hak istimewa hanya untuk layanan atau akun pengguna yang diperlukan dan lakukan pemantauan berkelanjutan jika terdapat aktivitas anomali;

- Menerapkan perimeter keamanan, seperti *firewall* berbasis *host* (*Host-based Firewall*), hal ini untuk mengelola perizinan koneksi ke pembagian administratif melalui *server message block* (SMB) dari sekumpulan mesin administrator terbatas;

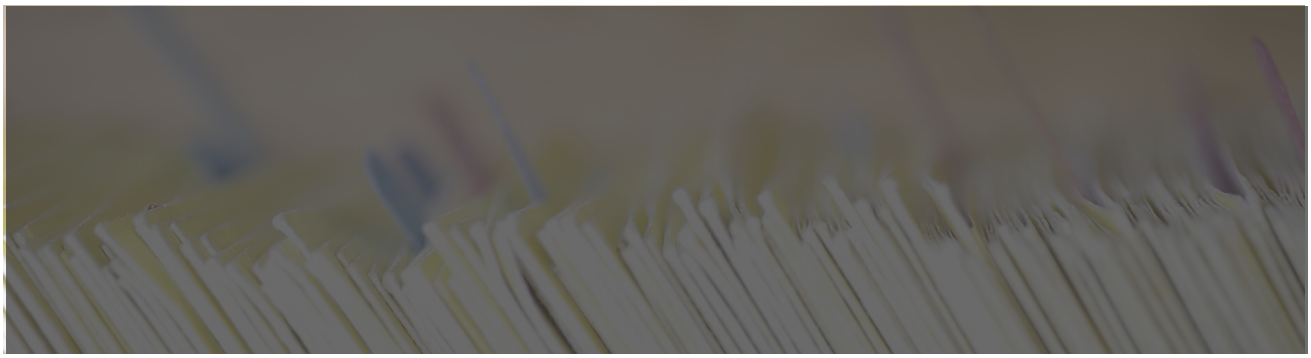
- Mengaktifkan file yang dilindungi di Sistem Operasi Windows untuk mencegah perubahan tidak sah pada *file* penting.

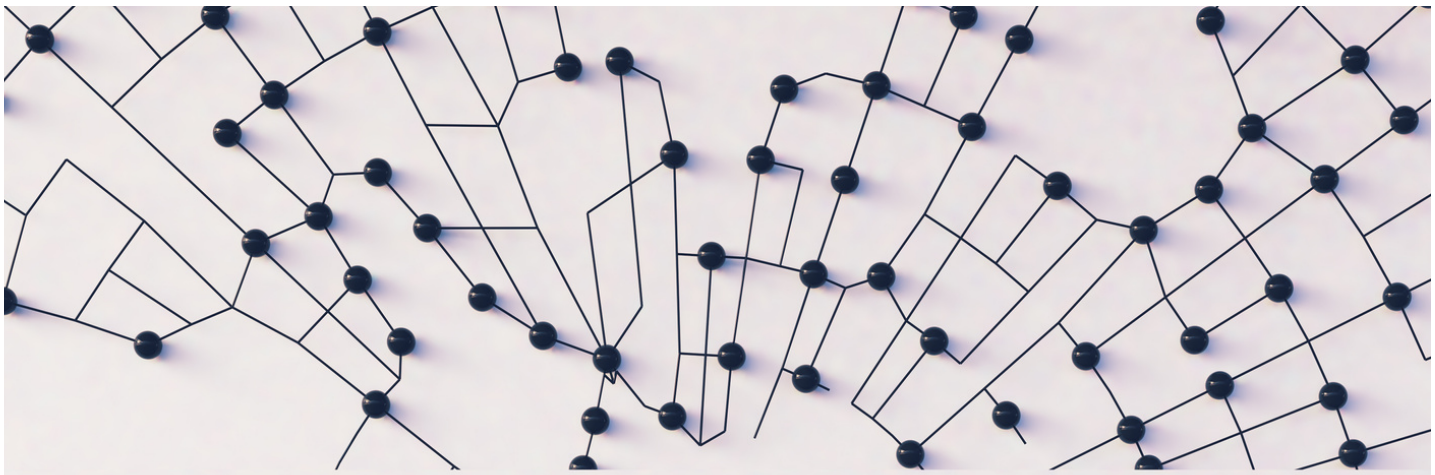
Penyerang atau pelaku ancaman menggunakan media *email* sebagai penyebaran malware serta menggunakan teknik *anti-VM* dan *anti-debugging* dengan melakukan pemindaian sistem dan jaringan untuk visibilitas dan pemetaan jaringan/sistem. Untuk membatasi perilaku penyerang, perlu dilakukan beberapa langkah pencegahan serta pembatasan sistem umum dan teknik yang digunakan penyerang:

- Melakukan pembaruan kredenial *email* secara berkala dengan password yang kuat;
- Tidak membuka tautan atau link *email* yang meragukan untuk menghindari phishing;
- Melakukan segmentasi jaringan untuk mencegah penyebaran *malware*. Hal ini dapat membantu karena dengan segmentasi jaringan, arus lalu lintas antara dan akses ke berbagai subjaringan terkontrol dan membatasi pergerakan lateral penyerang.;
- Melakukan identifikasi, deteksi, dan penyelidikan aktivitas tidak wajar (abnormal) dan potensi traversal *malware* yang ditemukan menggunakan alat pemantauan jaringan. Alat ini akan mencatat dan melaporkan semua lalu lintas jaringan, termasuk aktivitas pergerakan lateral di jaringan. Contohnya dengan *endpoint detection and response* (EDR), alat ini berguna untuk mendeteksi koneksi lateral karena memiliki wawasan tentang koneksi jaringan umum dan tidak umum untuk setiap *host;*
- Menerapkan akses berbasis waktu (*session*) untuk akun yang disetel di tingkat admin dan yang lebih tinggi. Misalnya, metode akses *Just-in-Time* (JIT) menyediakan akses istimewa bila diperlukan dan dapat mendukung penegakan prinsip paling tidak istimewa (serta model *Zero Trust*);
- Menonaktifkan aktivitas dan izin *command line* dan *script.* Hal ini dikarenakan peningkatan hak istimewa dan pergerakan lateral sering kali bergantung pada utilitas perangkat lunak yang dijalankan dari baris perintah. Jika dinonaktifkan, pelaku ancaman akan mengalami kesulitan untuk meningkatkan hak istimewa dan/atau melakukan pergerakan lateral;
- Selalu melakukan pencadangan data *offline* dan pemulihan cadangan data secara teratur;
- Memastikan semua data cadangan dienkripsi, tidak dapat diubah (yaitu, tidak dapat diubah atau dihapus) dan mencakup seluruh infrastruktur data organisasi.

Referensi

- https://www.hybrid-analysis.com/sample/f4ba5e8f98fe70d764df71b7c390237b90ed0fc3408579a15a06ee56008a3531
- https://www.virustotal.com/gui/file/f4ba5e8f98fe70d764df71b7c390237b90ed0fc3408579a15a06ee56008a3531/community
- https://blog.morphisec.com/threat-alert-mylobot-new-sophisticated-botnet
- https://www.deepinstinct.com/blog/meet-mylobot-a-new-highly-sophisticated-never-seen-before-botnet-thats-out-in-the-wild
- https://www.makeuseof.com/tag/download-operation-cleanup-complete-malware-removal-guide/
- https://www.prosyscom.tech/tips-tricks/what-is-mylobot-malware-how-it-works-and-what-to-do-about-it-tips-tricks/
- https://www.darkreading.com/vulnerabilities-threats/mylobot-malware-brings-new-sophistication-to-botnets
- https://blog.minerva-labs.com/mylobot-2022-so-many-evasive-techniques-just-to-send-extortion-emails
- https://malpedia.caad.fkie.fraunhofer.de/details/win.mylobot
- https://thehackernews.com/2022/02/new-mylobot-malware-variant-sends.html





Direktorat Operasi Keamanan Siber

BADAN SIBER DAN SANDI NEGARA

(021)78833610
bantuan70@bssn.go.id / www.idsirtii.or.id
Jl. Harsono RM No. 70, Ragunan, Pasar Minggu,
Jakarta Selatan, 12550