2026

SECURITY REPORT

Unauthorized External Command and Control Traffic Detected

github.com/Abdibimantara abdibimantara.github.io abdibimantara91@gmail.com

Table of Contents

Executive Summary

- Incident ID : INC-20260122-ItSecurity
- Incident Severity : **Medium**
- Incident Overview

  Tim Security Operations Center (SOC) berhasil menidentifikasi terkait dengan adanya aktivitas anomali pada environment internal perusahaan. Berdasarkan hasil temuan melalui log traffic menunjukkan adanya indikasi command and control (C2) connection. Hal ini diperkuat dengan adanya aktivitas downloading dari IP internal yang melibatkan sejumlah suspicious executable file. Temuan tersebut menunjukkan adanya potensi sistem tercompromised, sehingga perlu dilakukan tindakan respons serta investigasi lebih lanjut.

- Key Findings :

  Ditemukan adanya aktivitas outbound connection dari IP addresss 147.32.84[.]165 ke arah IP address eksternal yaitu 195.88.191[.]59 yang terindikasi sebagai malicious IP. Dilihat dari behavior connection tersebut tidak termasuk dalam authorized connection. Temuan terkait dengan outbound connection tersebut terlihat berulang dalam rentang waktu yang berdekatan, sehingga terindikasi adanya komunikasi terhadap Command and Control IP ataupun Domain. Penelusuran lebih detail, mendapati adanya beberapa file executable yaitu chooseee.exe, fjuivgfhurew.exe, client.exe, 3425.exe, kx4.txt yang melalui domain nocomcom[.]com. Validasi terhadap file executable tersebut, berdasarkan indikator teknis seperti File Hash, Signature ataupun Reputation Source, mengonfirmasi bahwa artefak tersebut diklasifikasikan sebagai malicious. Seluruh temuan diperoleh melalui korelasi log lalu lintas jaringan yang bersumber dari Suricata dan Zeek, yang digunakan untuk memvalidasi pola komunikasi jaringan, aktivitas pengunduhan, serta keterkaitan antara host internal dan infrastruktur eksternal yang terlibat dalam insiden.

- Immediate Actions :

  Tim Security Operations Center (SOC) secara aktif melakukan analisa terstruktur terkait dengan indikais adanya command and control (C2) yang berasal dari devcie tercompromised. IP Address serta malicious domain yang teridentifikasi segera diblokir guna mencegah adanya komunikasi berlanjut. Untuk mendukung proses investigasi dan validasi temuan, log traffic dari Suricata serta Zeek diamankan untuk dipantau secara berkelanjutan. Selain itu, dilakukan monitoring intensif terhadap aktivitas jaringan dan host terkait untuk mendeteksi indikasi lanjutan dari kompromi atau penyebaran ancaman tambahan.

- Stakeholder Impact :

  Insiden ini berpotensi memengaruhi beberapa stakeholder yang bergantung pada sistem dan jaringan informasi perusahaan, khususnya unit kerja yang terkait dengan aset informasi [Asset Name / System Name] yang berada di bawah tanggung jawab [Asset Owner / Unit Owner]. Aktivitas komunikasi tidak sah dengan infrastruktur eksternal serta pengunduhan file executable berbahaya menimbulkan risiko terhadap aspek kerahasiaan, integritas, dan ketersediaan (CIA) aset informasi tersebut. Berdasarkan penilaian risiko

sementara, insiden ini diklasifikasikan memiliki tingkat dampak Medium, dengan mempertimbangkan potensi gangguan operasional dan eksposur keamanan informasi. Risiko yang teridentifikasi telah dicatat dan ditelusurkan dalam risk register organisasi dengan referensi [Risk ID / Risk Register Reference], serta dikelola sesuai dengan kebijakan manajemen risiko dan prosedur penanganan insiden keamanan informasi yang berlaku.

Technical Analysis

Pada tahap analisis teknis ini, tim Security Operations Center (SOC) belum memiliki akses langsung terhadap log endpoint sehingga belum dapat melakukan verifikasi terkait aktivitas pada host yang memicu terjadinya komunikasi jaringan mencurigakan. Secara paralel, koordinasi sedang dilakukan dengan tim pengelola endpoint untuk memperoleh log endpoint yang relevan guna mendukung analisis lanjutan dan memastikan pemahaman yang komprehensif terhadap sumber dan mekanisme aktivitas tersebut.

- ### Affected Systems & Data :

  Sistem yang terdampak dalam insiden ini mencakup asset internal 147.32.84[.]165 yang teridentifikasi melakukan komunikasi outbound ke infrastruktur eksternal berbahaya serta aktivitas pengunduhan file executable. Diketahui bawa IP address tersebut merupakan bagian dari aset internal perusahaan yang digunakan karyawan. Hingga tahap pelaporan ini, belum terdapat indikasi terkonfirmasi mengenai akses tidak sah, perubahan, atau kehilangan data sensitif. Namun demikian, potensi paparan terhadap data operasional masih dalam proses evaluasi lebih lanjut seiring dengan berjalannya analisis teknis lanjutan.

- ### Evindece Source & Analysis :

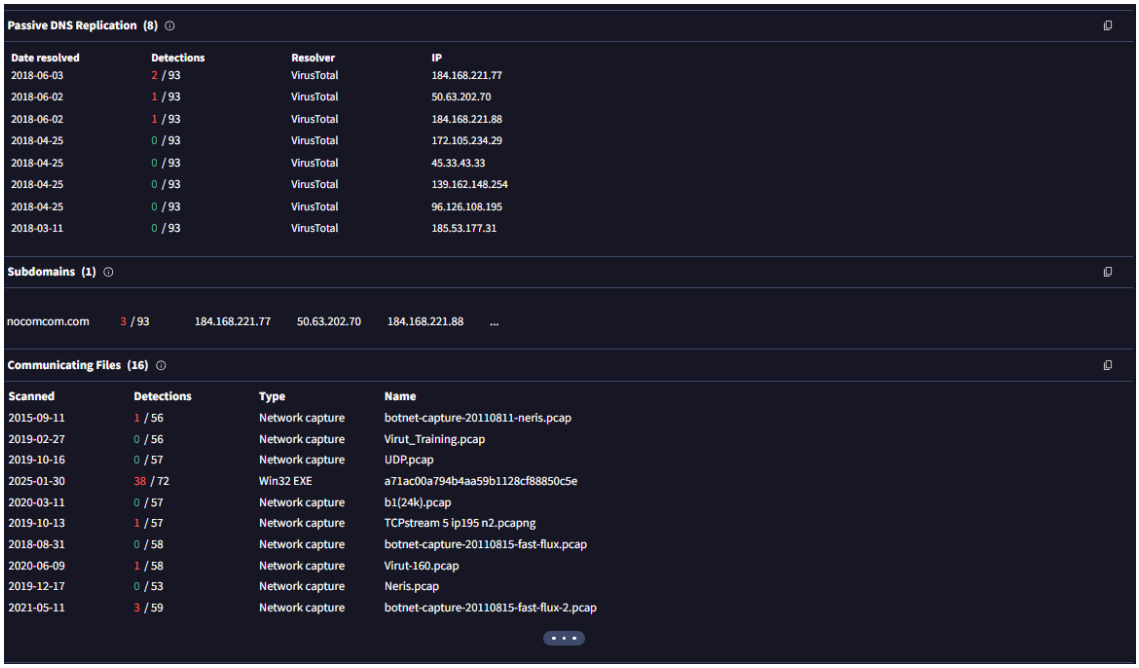
  Tim SOC mendapati pertama kali malicious activity dimulai pada jam 09:01. Dimana diketahui adanya aktivitas koneksi outbound dari asset intenal perusahaan yaitu 147.32.84[.]165 kearah IP eksternal yaitu 195.88.191[.]59.

_time	src_ip	dest_ip	dest_port	signature	http.url	http.hostname
2011-08-10 09:01:40.475	147.32.84.165	195.88.191.59	80			
2011-08-10 09:01:40.475	147.32.84.165	195.88.191.59	80		/temp/3425.exe?t=0.3419458	nocomcom.com
2011-08-10 09:01:40.475	195.88.191.59	147.32.84.165	1052		/temp/3425.exe?t=0.3419458	nocomcom.com
2011-08-10 09:06:50.920	195.88.191.59	147.32.84.165	1042	SURICATA TCPv4 invalid checksum	/kx4.txt	nocomcom.com
2011-08-10 09:06:51.998	195.88.191.59	147.32.84.165	1042	SURICATA TCPv4 invalid checksum	/kx4.txt	nocomcom.com
2011-08-10 09:06:52.652	195.88.191.59	147.32.84.165	1042	SURICATA TCPv4 invalid checksum	/kx4.txt	nocomcom.com
2011-08-10 09:06:52.653	195.88.191.59	147.32.84.165	1042	SURICATA TCPv4 invalid checksum	/kx4.txt	nocomcom.com
2011-08-10 09:06:52.675	195.88.191.59	147.32.84.165	1042	SURICATA TCPv4 invalid checksum	/kx4.txt	nocomcom.com
2011-08-10 09:06:52.847	195.88.191.59	147.32.84.165	1042	SURICATA TCPv4 invalid checksum	/kx4.txt	nocomcom.com
2011-08-10 09:06:53.232	147.32.84.165	195.88.191.59	80		/kx4.txt	nocomcom.com

  Koneksi tersebut juga diketahui berhubungan dengan HTTP service spesifik port 80 yang bersifat suspicious. Selain itu tim SOC juga menemukan bahwa terdapat domain yang berjalan melalui IP address tersebut yaitu nocomcom[.]com, konfirmasi dari tim internal perusahaan domain tersebut tidak termasuk dalam whitelist.

Communicating Files (7)

Scanned	Detections	Type	Name
2019-10-16	0 / 57	Network capture	UDP.pcap
2013-08-27	3 / 46	Network capture	93F8557D29BAD3AC50FC75EF5B9D00CCC27CFD09911DEE706D446C68CCE60B01
2020-06-09	1 / 58	Network capture	Virut-160.pcap
2013-08-16	0 / 46	Network capture	A5C1524C8D62E326FF8BF5D13DF0BD31729840A432FFBD954F5148ADD8CE2F8B
2013-08-16	2 / 46	Network capture	AABA87A16C174F5C86C54AF0F5221C43785067F2B79BA6CF4D67656E4ECE17D2
2023-10-31	0 / 60	Network capture	nouveauPCAP.pcap
2013-08-25	2 / 45	Network capture	CFC3A84EB33B4BB2E2AF43AC0AA9213CBBD05A54E1B4826E29AF7608466F7A2D



Passive DNS Replication (8)

Date resolved	Detections	Resolver	IP
2018-06-03	2 / 93	VirusTotal	184.168.221.77
2018-06-02	1 / 93	VirusTotal	50.63.202.70
2018-06-02	1 / 93	VirusTotal	184.168.221.88
2018-04-25	0 / 93	VirusTotal	172.105.234.29
2018-04-25	0 / 93	VirusTotal	45.33.43.33
2018-04-25	0 / 93	VirusTotal	139.162.148.254
2018-04-25	0 / 93	VirusTotal	96.126.108.195
2018-03-11	0 / 93	VirusTotal	185.53.177.31

Subdomains (1)

nocomcom.com 3 / 93 184.168.221.77 50.63.202.70 184.168.221.88 ...

Communicating Files (16)

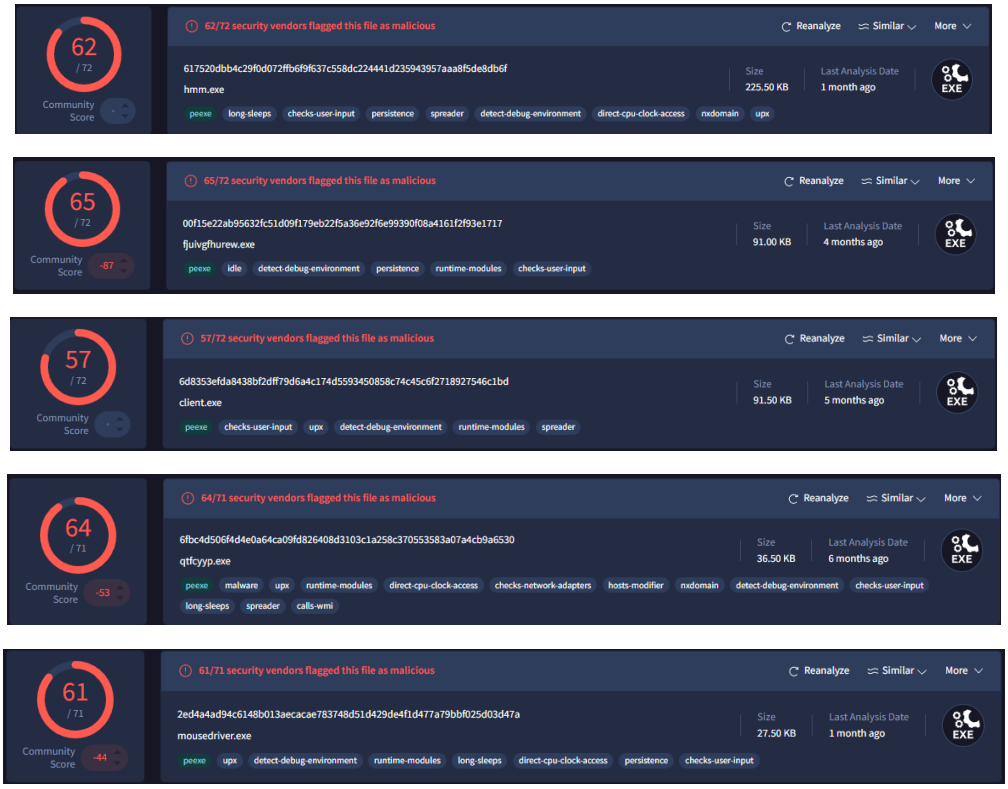
Scanned	Detections	Type	Name
2015-09-11	1 / 56	Network capture	botnet-capture-20110811-neris.pcap
2019-02-27	0 / 56	Network capture	Virut_Training.pcap
2019-10-16	0 / 57	Network capture	UDP.pcap
2025-01-30	38 / 72	Win32 EXE	a71ac00a794b4aa59b1128cf88850c5e
2020-03-11	0 / 57	Network capture	b1(24k).pcap
2019-10-13	1 / 57	Network capture	TCPstream 5 ip195 n2.pcapng
2018-08-31	0 / 58	Network capture	botnet-capture-20110815-fast-flux.pcap
2020-06-09	1 / 58	Network capture	Virut-160.pcap
2019-12-17	0 / 53	Network capture	Neris.pcap
2021-05-11	3 / 59	Network capture	botnet-capture-20110815-fast-flux-2.pcap

Validasi dilakukan oleh tim SOC melalui Indicator of Compromised (IoC) yang berhasil diketahui, IP Address menunjukkan adanya hubungan antara IP Address tersebut terhadap beberapa file executable yang terindikasi sebagai Malicious. Selain itu Untuk domain yang terhubung dengan IP Address tersebut valid terdeteksi sebagai malicious.

_time	src_ip	dest_ip	eventtype	url
2011-08-10 11:02:41.341	147.32.84.165	195.88.191.59	suricata_eve_http	/bl/chooseee.exe?t=0.8925135
2011-08-10 11:02:21.972	147.32.84.165	195.88.191.59	suricata_eve_http	/sv/fjuivgfhurew.exe?t=0.3069879
2011-08-10 11:02:11.688	147.32.84.165	195.88.191.59	suricata_eve_http	/bl/client.exe?t=0.9562799
2011-08-10 10:10:32.255	147.32.84.165	195.88.191.59	suricata_eve_http	/kx4.txt
2011-08-10 09:01:40.475	147.32.84.165	195.88.191.59	suricata_eve_http	/temp/3425.exe?t=0.3419458

Observasi yang dilakukan oleh tim SOC mendapati dari koneksi kearah IP Address external tersebut melibatkan beberapa file executable (Download). Secara behavior, aktivitas download tersebut sudah termasuk malicious bagi internal perusahaan, namun validasi tetep dilakukan oleh tim SOC melalui log Zeek. Dimana korelasi antara log suricata dan Zeek berdasarkan field unique id dan File unique id.

Executable Name	Md5 Sum
chooseee.exe	7c8d12f776b17da6576c6469d8ad5a2b
fjuivgfhurew.exe	42d00e295e1c3715acd51a0fc54bad87
client.exe	8ed68a129b3634320780719abf6635cc
kx4.txt	564048b35da9d447f2e861d5896d908d
3425.exe	a7d0e9196d472dbaa6948fdeb33045a0



Hasil validasi Hash melalui Virtustotals, menunjukkan bahwa executable tersebut masuk dalam kategori trojan. Hal ini membuktikan bahwa aktivitas outbound tersebut termasuk dalam aktivitas suspicious.

- Indicator of Compromise (IoCs) :
  - Malicious IP : 195.88.191[.]59
  - Malicious Domain : nocomcom[.]com
  - Malicious Hash : c8d12f776b17da6576c6469d8ad5a2b
    42d00e295e1c3715acd51a0fc54bad87
    8ed68a129b3634320780719abf6635cc
    564048b35da9d447f2e861d5896d908d
    a7d0e9196d472dbaa6948fdeb33045a0

- Root Cause Analysis :

  Berdasarkan hasil analisa melalui SIEM, aktivitas ini dimulai dari outbound connection yang berasal dari asset internal perusahaan 147.32.84[.]165 ke malicious IP melalui service HTTP dengan spesifik port 80, yang berhubungan dengan process downloading file executable. Validasi terhadap IoC menunjukkan bahwa IP Address serta Domain eksternal memiliki reputasi malicious, sementara artefak yang diunduh diklasifikasikan sebagai trojan berdasarkan hasil analisis hash menggunakan VirusTotal. Pada tahap pelaporan ini, keterbatasan visibilitas terhadap log endpoint membatasi kemampuan untuk mengidentifikasi secara pasti aktivitas awal pada host yang memicu komunikasi tersebut, sehingga penentuan vektor awal kompromi memerlukan analisis lanjutan terhadap data endpoint yang relevan.

- Technical Timeline :
    - **09:01:00 — Initial Detection (Command and Control)**
      Sistem monitoring jaringan mendeteksi koneksi outbound dari aset internal **147.32.84[.]165** menuju IP eksternal **195.88.191[.]59** melalui HTTP port 80.
      MITRE ATT&CK: *Command and Control – Application Layer Protocol (T1071.001)*
    - **09:01:05 – 09:02:30 — Sustained C2 Communication**
      Teridentifikasi komunikasi HTTP berulang dengan pola yang konsisten dan menyimpang dari baseline lalu lintas normal, mengindikasikan komunikasi terarah dengan infrastruktur eksternal tidak sah.
      MITRE ATT&CK: *Command and Control – Beaconing (T1071)*
    - **09:02:45 — Malicious Domain Interaction**
      Host internal mengakses domain **nocomcom[.]com**, yang tidak termasuk dalam whitelist internal dan terasosiasi dengan infrastruktur berbahaya.
      MITRE ATT&CK: *Command and Control – Dynamic Resolution (T1568)*
    - **09:03:10 — Payload Retrieval**
      Terobservasi aktivitas pengunduhan beberapa file executable dari infrastruktur eksternal ke host internal melalui sesi HTTP.
      MITRE ATT&CK: *Command and Control – Ingress Tool Transfer (T1105)*
    - **09:04:00 – 09:06:00 — Evidence Correlation**
      Korelasi log Suricata dan Zeek mengonfirmasi hubungan antara koneksi outbound, domain tujuan, dan file executable yang diunduh berdasarkan **flow identifier** dan **file unique identifier**.
      MITRE ATT&CK: *Command and Control – Application Layer Protocol (T1071.001)*
    - **09:10:00 — Malware Classification**
      Validasi hash file executable menunjukkan artefak diklasifikasikan sebagai **trojan** berdasarkan analisis reputasi menggunakan VirusTotal.
      MITRE ATT&CK: *Command and Control – Ingress Tool Transfer (T1105)*
    - **09:15:00 — Containment Action**
      Aktivitas komunikasi outbound ke infrastruktur eksternal berbahaya dihentikan melalui penerapan langkah kontainmen dan pemantauan lanjutan oleh tim SOC.
      MITRE ATT&CK: *Mitigation – Network Traffic Filtering (M1037)*

- Nature of the Attack

  Observed Behavior

  Teridentifikasi outbound connection dari host internal **147.32.84[.]165** menuju IP eksternal **195.88.191[.]59** melalui service HTTP pada port 80, termasuk interaksi dengan domain **nocomcom[.]com** yang tidak terdaftar whitelist. Pola traffic yang diamati menunjukkan koneksi berulang dengan karakteristik terstruktur, serta aktivitas downloading beberapa file executable dari sumber eksternal. Validasi terhadap IoC mengonfirmasi bahwa file executable tersebut memiliki reputasi malicious dan diklasifikasikan sebagai **trojan** berdasarkan hasil analisis hash menggunakan VirusTotal.

  Assessed Technique (MITRE ATT&CK)

  Berdasarkan behavior analysus, aktivitas ini dinilai konsisten dengan taktik **Command and Control** (TA0011) MITRE ATT&CK, khususnya teknik Application Layer Protocol Web Protocols (T1071.001) dan Dynamic Resolution (T1568) yang digunakan untuk

mempertahankan komunikasi dengan infrastruktur eksternal. Aktivitas downloading executable file selanjutnya sejalan dengan pemanfaatan teknik Ingress Tool Transfer (T1105). Penilaian ini dilakukan berdasarkan korelasi bukti jaringan dan indikator teknis yang tersedia, dan bersifat tentatif hingga dilakukan validasi lanjutan melalui data endpoint.

Impact Analysis

Temuan ini berpotensi berdampak terhadap **kerahasiaan, integritas, dan ketersediaan (CIA)** aset informasi yang terkait dengan host internal **147.32.84[.]165**, khususnya akibat adanya unathorized communication terhadap IP eksternal berbahaya dan malicious downloading file executable. Meskipun hingga tahap pelaporan ini belum terdapat bukti terkonfirmasi mengenai akses unauthorized, perubahan, ataupun data eksfiltration, keberadaan malware trojan pada endpoint berpotensi memungkinkan aktivitas lanjutan seperti remote command execution, malicious payload deployment, atau misuse of system resources. Dampak terhadap operasional bisnis dan layanan pengguna saat ini dinilai **terbatas**, namun risiko eskalasi tetap ada apabila aktivitas berbahaya tidak sepenuhnya dimitigasi, sehingga pemantauan lanjutan dan validasi teknis tambahan diperlukan untuk memastikan stabilitas dan keamanan lingkungan secara menyeluruh.

Response and Recovery Analysis

- ### Immediate Response Actions :

  Tim SOC segera melakukan identifikasi dan validasi awal terhadap indikator kompromi (IOC) yang terdeteksi dari sumber log jaringan dan keamanan perimeter. Langkah containment awal diterapkan dengan membatasi komunikasi jaringan mencurigakan untuk mencegah potensi eskalasi insiden. Secara paralel, koordinasi dilakukan dengan tim terkait untuk pengumpulan artefak tambahan guna mendukung analisis lanjutan.

- ### Eradication Measures :

  Setelah indikator ancaman terkonfirmasi, langkah eradikasi dilakukan dengan memastikan artefak berbahaya diisolasi dan dihapus dari environmen terdampak. Proses ini mencakup penonaktifan mekanisme persistensi yang teridentifikasi, validasi integritas sistem, serta penerapan kontrol keamanan tambahan untuk mencegah re-infeksi atau pemanfaatan ulang vektor serangan yang sama.

- ### Recovery Steps :

  Tahap pemulihan dilakukan dengan mengembalikan sistem ke kondisi operasional yang aman dan terkendali. Seluruh konfigurasi keamanan diverifikasi ulang untuk memastikan kesesuaian dengan baseline yang telah ditetapkan. Sistem yang terdampak dipantau secara ketat setelah pemulihan guna memastikan tidak terdapat aktivitas anomali lanjutan sebelum dinyatakan kembali beroperasi secara normal.

- Post-Incident Actions :

Monitoring

Pasca insiden, pemantauan berkelanjutan diterapkan terhadap sistem dan jaringan terkait dengan fokus pada IOC, pola lalu lintas mencurigakan, serta teknik serangan yang relevan. Penyesuaian use case dan rule deteksi dilakukan untuk meningkatkan kemampuan deteksi dini terhadap aktivitas serupa di masa mendatang.

Lessons Learned

Evaluasi pasca insiden dilakukan untuk mengidentifikasi celah pada kontrol teknis, proses operasional, maupun koordinasi antar tim. Hasil evaluasi ini digunakan sebagai dasar peningkatan prosedur respons insiden, penguatan kontrol keamanan, serta peningkatan kesiapan organisasi dalam menghadapi ancaman siber yang sejenis di kemudian hari.