NOVACAINE.
ARCANA IMPERII

Tentang Laporan Ini

Ini hasil riset berbasis data & fakta yang dirancang untuk membuka wawasan tentang isu-isu penting!

Catatan Penting

Bukan opini institusi atau laporan resmi! Semua isi murni perspektif penulis berdasarkan riset.

PUBLICATION PAPER

INSIGHT Opening Insights into Public Security and Information

Desember 12, 2024

ISTOCK

FiveBears Operations - Russian Hackers Group in the Kremlin

Candra Ihsan

Artikel ini mengkaji operasi siber yang dilakukan oleh kelompok Advanced Persistent Threat (APT) yang berafiliasi dengan badan intelijen Rusia, termasuk GRU, SVR, dan FSB. Sejak 1990-an, Rusia telah menggunakan operasi siber untuk spionase, sabotase, dan pengaruh global. Kelompok utama seperti Fancy Bear (APT28), Cozy Bear (APT29), Venomous Bear (Turla), Energetic Bear (Dragonfly), dan Voodoo Bear (Sandworm) menargetkan pemerintah, sektor energi, infrastruktur kritis, serta organisasi politik. Serangan mereka mencakup peretasan pemilu AS 2016, malware destruktif NotPetya, serta infiltrasi jaringan energi global. Dengan teknik canggih dan strategi false flag, kelompok ini sulit diidentifikasi dan terus berkembang. Operasi mereka mendukung kebijakan luar negeri Rusia dan memperkuat posisi geopolitiknya. Studi ini menyoroti bagaimana ancaman siber Rusia memengaruhi keamanan global dan menekankan perlunya respons yang efektif terhadap serangan yang semakin kompleks.

Origin and Connectivity with Intelligence Agencies

Tahun 90-an, Rusia telah melakukan berbagai operasi siber berbahaya, mulai dari spionase (mencuri informasi rahasia) hingga sabotase (menghancurkan atau mengganggu sistem). Salah satu operasi awal yang terkenal adalah serangan Moonlight Maze pada tahun 1996, yang menjadi titik awal jaringan operasi siber kompleks yang dikaitkan dengan Rusia. Saat ini, kelompok-kelompok ancaman yang didukung oleh pemerintah Rusia membentuk jaringan yang terorganisir dan sangat terampil, dengan operasi yang mencakup skala global. Tujuan mereka meliputi mendukung kebijakan luar negeri Rusia, menghalangi lawan, mencegah eskalasi konflik, hingga membantu Rusia menangani konflik secara strategis. Operasi siber ini telah menjadi elemen penting dalam strategi kekuatan global Rusia.

Namun, mengidentifikasi kelompok-kelompok ini adalah tantangan besar. Mereka sering kali mengubah alat dan metode serangan mereka, atau bahkan berbagi alat dengan kelompok lain. Akibatnya, informasi tentang operasi ini bisa berubah sewaktu-waktu berdasarkan temuan baru. Perusahaan keamanan siber juga sering menggunakan nama yang berbeda untuk kelompok yang sama, sehingga sulit untuk menyamakan laporan tentang mereka. Meskipun begitu, kelompok ini tetap menjadi ancaman serius yang terus berkembang. [1]

Fancy Bear

Kelompok peretas terkenal yang diduga kuat bekerja di bawah naungan Direktorat Intelijen Utama Rusia (GRU), khususnya Unit GTsSS 26165 [2]; [3]. Kelompok ini menjadi sorotan global karena keterlibatannya dalam mengganggu pemilu presiden Amerika Serikat pada tahun 2016. Fancy Bear memiliki sumber daya yang besar dan dikenal gigih dalam melaksanakan serangan sibernya. Selain Amerika Serikat, kelompok ini juga melakukan operasi berbahaya di Eropa, dan belakangan memperluas targetnya ke wilayah timur [4]. Fancy Bear telah aktif setidaknya sejak tahun 2004, menjadikannya salah satu aktor siber yang paling berpengalaman. Kelompok ini juga dikenal dengan berbagai nama lain yang digunakan oleh perusahaan keamanan siber, termasuk Sofacy, APT28, Sednit, Pawn Storm, Group 74, Tsar Team, Strontium, Swallowtail, SIG40, Grizzly Steppe, TG-4127, dan SNAKEMACKEREL. Nama-nama tersebut sering kali muncul dalam laporan yang mendokumentasikan aktivitas mereka, mencerminkan jangkauan luas operasi Fancy Bear di dunia maya.

Target Spesifik : pemerintah, partai politik, organisasi senjata anti-kimia, organisasi anti-doping, sektor energi, dan institusi pendidikan.

Gambar 1. Daftar FBI yang diinginkan dari perwira intelijen militer Rusia yang terhubung dengan GRU. Sumber: Biro Investigasi Federal

Cozy Bear

Sama halnya dengan si Fancy, kelompok peretas ini sangat terorganisir dan memiliki sumber daya besar dengan dedikasi yang tinggi, sangat berkaitan erat dengan Dinas Intelijen Asing Rusia (SVR) [5]. Fokus utama Cozy Bear adalah spionase siber, yakni mengumpulkan informasi intelijen dari seluruh dunia untuk mendukung kebijakan keamanan Rusia. Kelompok ini telah dikaitkan dengan pemerintah Rusia setidaknya sejak tahun 2008 [2]. Salah satu ciri khas Cozy Bear adalah kemampuan mereka untuk terus berupaya mendapatkan akses ke jaringan target tertentu, bahkan setelah kehilangan kendali operasional [5].

Dikenal dengan berbagai nama lain, tergantung pada sumber atau perusahaan keamanan siber yang merujuk pada kelompok ini. Beberapa nama lain yang digunakan untuk Cozy Bear antara lain APT29, Dukes, Group 100, Cozy Duke, EuroAPT, CozyCar, Cozer, Minidionis, SeaDuke, dan Hammer Toss.

Target Spesifik : pemerintah, lembaga penelitian, lembaga pemikir (think tank), dan organisasi politik.

Venomous Bear

Venomous Bear, juga dikenal dengan banyak nama lain seperti Turla Group, Snake, dan Waterbug, adalah kelompok aktor siber yang sangat termotivasi dan berfokus pada pengumpulan intelijen diplomatik. Kelompok ini diduga kuat didukung oleh kemampuan Signals Intelligence (SIGINT) yang memiliki keterkaitan dengan Dinas Keamanan Federal Rusia (FSB) [3]. Aktif sejak setidaknya tahun 2004 [2], Venomous Bear dikenal karena kemampuannya yang luar biasa dalam beradaptasi, menggunakan teknik-teknik baru dan canggih untuk menjaga keamanan operasional mereka. [6]

Dengan berbagai nama alias seperti Group 88, Krypton, Uroburos, hingga ITG12, kelompok ini terus menunjukkan fleksibilitas dan inovasi dalam dunia spionase siber, menjadikannya salah satu ancaman yang paling sulit dideteksi di dunia maya.

Target Spesifik : pemerintah, militer, institusi pendidikan, lembaga riset, sektor luar angkasa, telekomunikasi, dan perusahaan farmasi.

Energetic Bear

Kelompok aktor siber yang satu ini sangatlah canggih dan diduga beroperasi di bawah kendali Centre 16 milik FSB, badan intelijen Rusia [7] ; [3]. Kelompok ini dikenal karena menargetkan sektor-sektor yang dianggap strategis untuk kepentingan nasional. Sasaran utamanya mencakup instalasi energi, sumber daya minyak dan gas alam di Timur Tengah, serta peralatan komunikasi militer [8]. Energetic Bear telah aktif sejak setidaknya akhir tahun 2010, menunjukkan pola operasi yang konsisten dan terencana dengan baik [9].

Kelompok ini juga dikenal dengan berbagai nama lain, termasuk Dragonfly, Crouching Yeti, Group 24, Koala Team, Berserk Bear, Anger Bear, Dymalloy, Havex, PEACEPIPE, Fertger, TEMP.Isotope, dan ALLANITE.

Target Spesifik : pemerintah, sektor penerbangan, energi, sistem kontrol industri, dan infrastruktur kritis.

Gambar 2. Daftar peretas Rusia yang diinginkan FBI yang terhubung dengan FSB's Center 16. Biro Investigasi Federal

Voodo Bear

Salah satu kelompok Advanced Persistent Threat (APT) paling terkenal asal Rusia, yang dikenal karena

serangannya terhadap infrastruktur penting. Kelompok ini mendapat perhatian luas karena keterlibatannya dalam serangan terhadap jaringan listrik Ukraina pada tahun 2015 dan serangan siber NotPetya pada tahun 2017. Voodoo Bear diduga merupakan unit siber yang beroperasi di bawah kendali GRU, badan intelijen militer Rusia, tepatnya dari Main Centre for Special Technologies (GTsST) Unit 74455. Kelompok ini telah aktif setidaknya sejak tahun 2009 dan menjalankan operasi canggih, mulai dari spionase hingga serangan siber yang bersifat destruktif [10] ; [2].

Pada Maret 2022, para penyelidik hak asasi manusia dari UC Berkeley School of Law meminta Pengadilan Kriminal Internasional (ICC) di Den Haag untuk mempertimbangkan operasi kelompok ini sebagai penyerangan perang, khususnya terkait konflik di Ukraina [11].

Kelompok ini dikenal dengan berbagai nama lain, termasuk Sandworm Team, TEMP.Noble, Electrum, TeleBots, Black Energy, Hades, dan masih banyak lagi.

Target Spesifik : Sektor Energi Ukraina, pemerintah, organisasi senjata anti-kimia, partai politik dan kampanye, serta infrastruktur penting.

Russian APT Bear Group

Kelompok Five Bear APT (Advanced Persistent Threat) sering mengubah alat yang mereka gunakan, berbagi alat dengan kelompok lain, atau melakukan operasi bendera palsu (false flag) untuk menghindari pelacakan dan atribusi [2]. Hal ini membuat sulit untuk memastikan siapa yang bertanggung jawab atas serangan siber tertentu.

PURPOSE STRATEGIC :

Targeting Attack

Kelompok APT Rusia telah terbukti mampu melakukan serangan yang mengganggu infrastruktur penting milik lawan mereka. Serangan ini sering kali menggunakan malware yang dirancang untuk menargetkan sistem kontrol industri (Industrial Control Systems/ICS). Jika serangan ini berhasil, mereka dapat mendapatkan akses ke sistem yang terlindungi, memungkinkan tindakan yang bersifat destruktif. Selain itu, kelompok APT Rusia memiliki kemampuan untuk bertahan dalam jaringan yang sudah mereka retas tanpa terdeteksi dalam waktu lama, menggunakan berbagai teknik untuk mendapatkan akses awal [3].

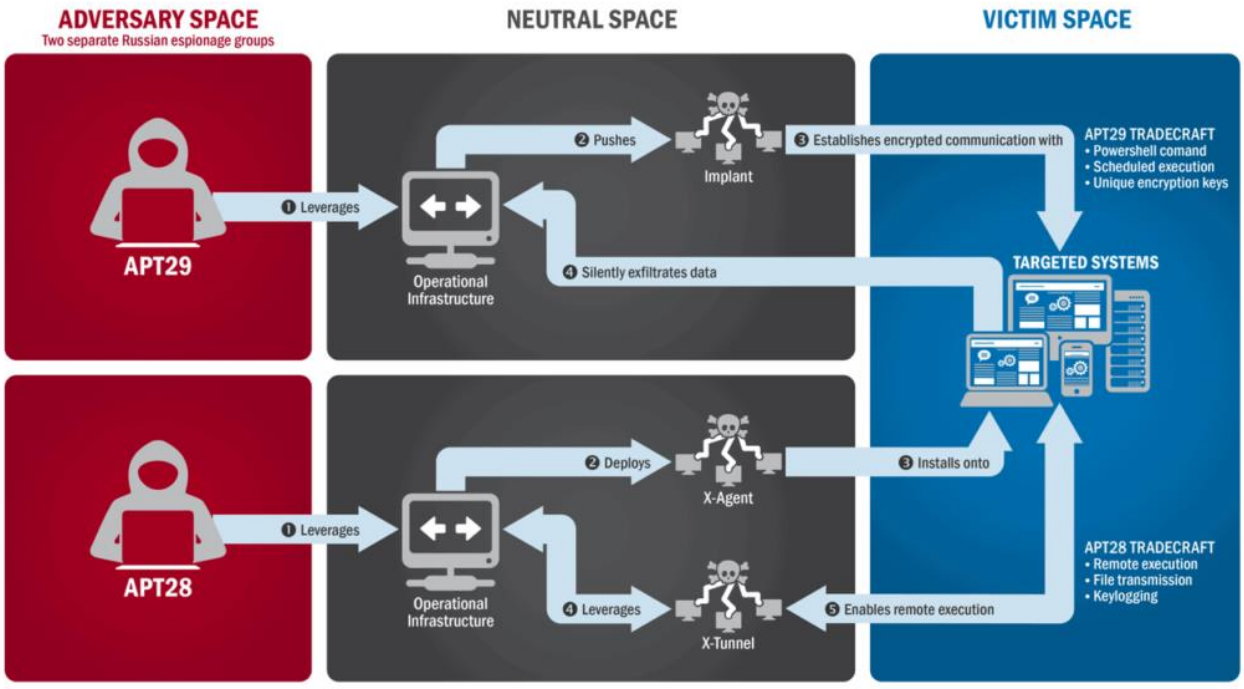
Espionage Operation

Kelompok APT yang terafiliasi dengan Rusia juga terlibat dalam spionase siber yang menargetkan sektor energi, penerbangan, transportasi, kesehatan, dan telekomunikasi. Operasi ini dikoordinasikan oleh badan intelijen Rusia untuk memenuhi berbagai tujuan, seperti mengembangkan kemampuan siber baru hingga mendukung kebijakan luar negeri Rusia [3].

Influence Operation

Selain serangan langsung, aktor siber yang didukung pemerintah Rusia juga berupaya melemahkan kepercayaan pada sistem demokrasi Barat. Mereka menggunakan media online rahasia dan outlet berita palsu untuk menyebarkan disinformasi. Selain itu, kelompok APT ini melakukan operasi yang menargetkan lembaga pemerintahan, memengaruhi pemilu nasional, dan membocorkan informasi sensitif seperti catatan

medis untuk menciptakan ketidakstabilan [3].



Gambar 3. Diagram dari Laporan AS-Cert tentang APT28 dan APT29 (alias Grizzly Steppe)-Gambar: Wikicommons

FIVE BEAR ACTION:

Serangan NotPetya

2017, lembaga keuangan dan pemerintah Ukraina menjadi target serangan siber besar yang dilakukan oleh aktor yang didukung pemerintah Rusia. Serangan ini menggunakan malware NotPetya, yang dikenal sebagai salah satu malware dengan penyebaran tercepat. Dengan memanfaatkan alat EternalBlue dan Mimikatz, malware ini mampu melewati celah keamanan pada sistem Windows, bahkan pada sistem yang sudah diperbarui (patched). Setelah satu perangkat terinfeksi, malware ini menyebar dengan sangat cepat, menghapus data penting di komputer korban dan membuat perangkat tidak dapat digunakan lagi.

Yang membedakan NotPetya adalah sifatnya yang murni destruktif—malware ini tidak dirancang untuk didekripsi atau dipulihkan, sehingga menjadikannya lebih seperti senjata penghancur daripada alat untuk pencurian data [10] ; [12].

Kampanye Intrusi Sektor Energi Global

Antara tahun 2011 hingga 2018, aktor siber yang didukung oleh pemerintah Rusia melancarkan kampanye serangan besar-besaran yang menargetkan jaringan sektor energi internasional. Dalam serangan ini, mereka terutama melakukan pengintaian untuk mempelajari sistem target dan meluncurkan malware yang dirancang khusus untuk menyerang Industrial Control Systems (ICS), yaitu sistem yang mengendalikan operasi penting dalam sektor energi. Serangan ini bertujuan untuk mengganggu, mencuri informasi, atau bahkan merusak infrastruktur energi yang menjadi tulang punggung banyak negara [13].

Serangan Jaringan Listrik Ukraina

Pada tahun 2015 dan 2016, kelompok APT (Advanced Persistent Threat) yang didukung oleh pemerintah Rusia melakukan serangan siber yang menargetkan perusahaan distribusi energi di Ukraina pada tahun 2015, dan perusahaan transmisi listrik pada tahun 2016. Akibat dari serangan ini, terjadi pemadaman listrik di beberapa wilayah, dan banyak komputer yang terinfeksi menjadi tidak dapat digunakan. Serangan ini menunjukkan kemampuan kelompok tersebut untuk mengganggu infrastruktur penting seperti jaringan listrik, yang berdampak langsung pada kehidupan masyarakat dan stabilitas negara [13].

Peretasan Pemilihan Presiden AS

2016, jaringan milik Komite Nasional Demokrat (DNC) di Amerika Serikat menjadi target serangan spear phishing, yaitu serangan siber yang menyasar individu atau organisasi tertentu melalui email palsu yang tampak meyakinkan. Serangan ini berhasil memberikan akses kepada pelaku untuk mendapatkan dokumen-dokumen yang berkaitan dengan pemilu. Insiden ini menjadi salah satu contoh bagaimana serangan siber dapat digunakan untuk memengaruhi proses politik [14] ; [3].

Referensi

[1] O. o. t. D. o. N. Intelligence, "ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY," 2021.

[2] A. Cristaldi, "APTMAP," Github, [Online]. Available: https://andreacristaldi.github.io/APTmap/#34.

[3] C. M. Centre, "SUBSTANTIVE REVISION: Russia: Cyber Threat Overview," OFFICE of INTELLIGENCE AND ANALYSIS, 2022.

[4] Great, "Masha and these Bears," SecureList, 09 3 2018. [Online]. Available: https://securelist.com/masha-and-these-bears/84311/.

[5] C. Strike, "Cozy Bear," CrowdStrike, [Online]. Available: https://www.crowdstrike.com/adversaries/cozy-bear/.

[6] C. Strike, "Venomous Bear," CrowdStrike, [Online]. Available: https://www.crowdstrike.com/adversaries/venomous-bear/.

[7] C. R. Service, "Russian Cyber Units," 2022.

[8] D. B. B. B. Z. C. J. E. K. B. M. M. M. K. A. J. C. P. H. B. I. A. G. D. A. C. F. E. S. F. E. O. Z. G. W. Pasquale Stirparo, "APT Groups and Operations," 2023. [Online]. Available: https://docs.google.com/spreadsheets/u/1/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml.

[9] K. L. G. R. a. A. Team, "Energetic Bear — Crouching Yeti," Kapersky, 2018.

[10] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[11] A. Greenberg, "The Case for War Crimes Charges Against Russia's Sandworm Hackers," Wired, 2022. [Online]. Available: https://www.wired.com/story/cyber-war-crimes-sandworm-russia-ukraine/.

[12] E. Nakashima, "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes," Washington Post, 2018. [Online]. Available: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

[13] A. C. D. Agency, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," 01 03 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a.

[14] D. P. Office, "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," Homeland Security, 07 October 2016. [Online]. Available: https://www.dhs.gov/archive/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.