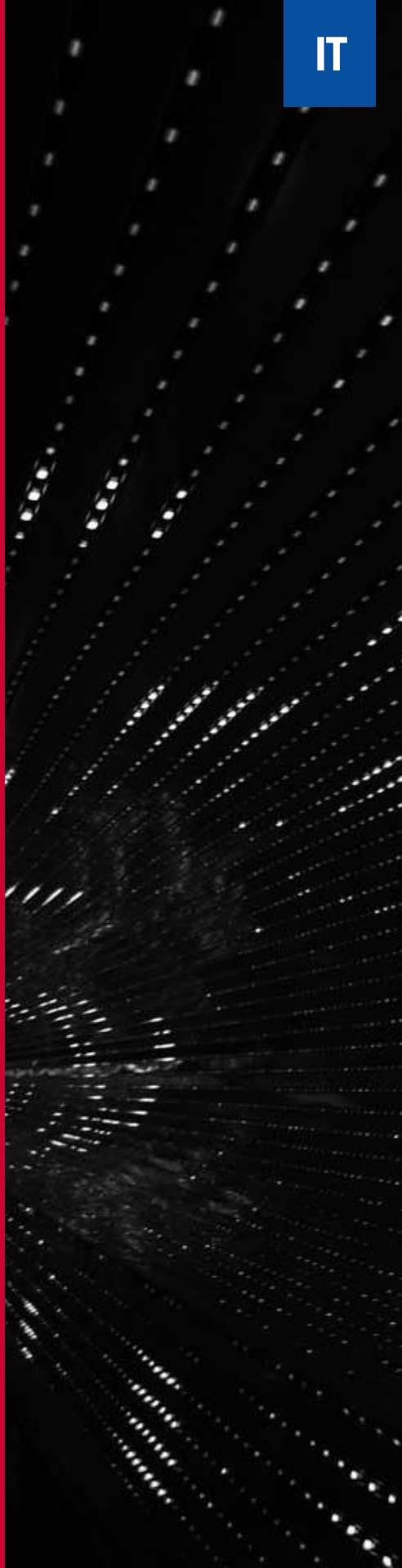
IT

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



Da gennaio 2019 ad aprile 2020

Botnet

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Una botnet è una rete di dispositivi collegati infettati da malware bot. Questi dispositivi sono in genere utilizzati da attori malintenzionati per lanciare attacchi distribuiti di negazione del servizio (Distributed Denial of Service, DDoS). Operando in modalità peer-to-peer (P2P)[1] o da un centro di comando e controllo (Command and Control, C2)[2], le botnet sono controllate a distanza da un attore malintenzionato per operare in modo sincronizzato al fine di ottenere un determinato risultato.[3]

I progressi tecnologici nel calcolo distribuito e nell'automazione hanno offerto ad attori malintenzionati l'opportunità di esplorare nuove tecniche e di migliorare strumenti e metodi di attacco. Grazie a ciò, le botnet operano in modi molto più distribuiti e automatizzati e sono disponibili presso fornitori self-service e pronti per l'uso.

Non solo i bot malevoli, denominati «bad bot», sono in continua evoluzione, ma le competenze delle persone e il livello di sviluppo dei bot stanno raggiungendo un elevato livello di specializzazione in alcune applicazioni, come fornitori di difesa o anche tecniche di elusione.[4] Da un punto di vista diverso, le botnet rappresentano un vettore che consente ai criminali informatici di lanciare varie operazioni, da frode legata all'e-banking a ransomware, cryptomining e attacchi DDoS.[5]

Risultati

7,7_milioni di dispositivi IoT sono collegati a Internet ogni giorno

Di questi, si stima che 1 su 20 sia protetto da un firewall o da strumenti di sicurezza di rete analoghi.[6]

57%_di aumento nel numero di varianti di Mirai rilevate nel corso del 2019

Sebbene le varianti di Mirai siano note per utilizzare tentativi di forza bruta prevalentemente per compromettere i dispositivi IoT, nel corso del 2019 si è osservato un aumento sia dei tentativi di forza bruta (51%) sia dello sfruttamento delle vulnerabilità dei siti web (87%).[7]

300 000_notifiche di traffico di botnet di Emotet durante il 2019

Queste sono state responsabili di oltre 100 000 segnalazioni di vittime in più rispetto allo stesso periodo del 2018. I ricercatori ritengono che vi sia stato un aumento del 913% del numero di campioni di Emotet, sulla base di un confronto fra il secondo semestre del 2018 e quello del 2019.[7]

60%_dell'attività della nuova botnet rivale è associata al furto delle credenziali[9]

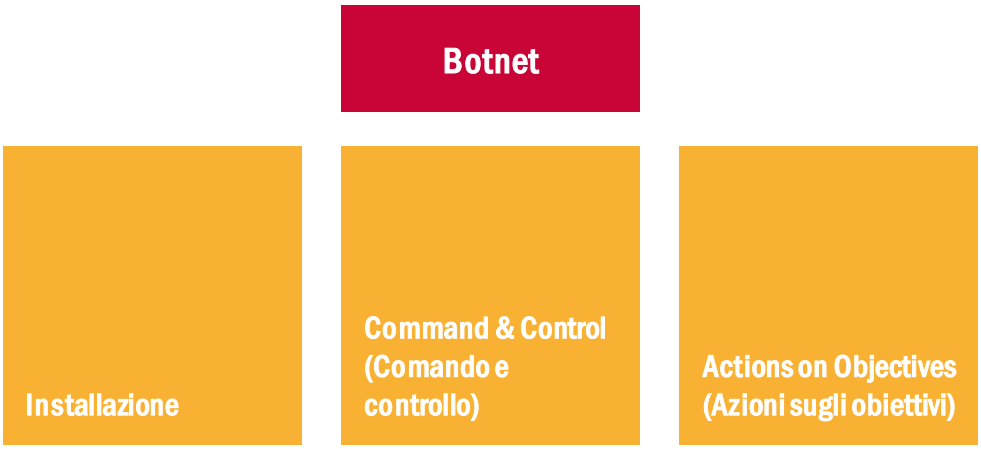
17 602_server C2 di botnet pienamente funzionali rilevati nel 2019

Aumento del 71,5% rispetto al 2018.[5]

Kill chain

Fase del flusso di lavoro dell'attacco

Ampiezza dello scopo



Il modello Cyber Kill Chain® è stato sviluppato da Lockheed Martin, che lo ha adattato da un concetto militare legato alla struttura di un attacco. Per studiare un particolare vettore di attacco si può utilizzare questo modello per mappare ogni fase del processo e fare riferimento agli strumenti, alle tecniche e alle procedure impiegate dall'aggressore.

MAGGIORI INFORMAZIONI

Tendenze

_I bot sono una miniera d'oro

I bot utilizzano capacità di forza bruta convincendo le vittime ad acquistare articoli in edizione limitata o in offerta promozionale e successivamente a rivenderli a un prezzo più alto. Questo fatto è stato individuato analizzando un annuncio di lavoro in cui l'inserzionista cercava uno sviluppatore di software con esperienza nell'aggirare le difese di sicurezza, creando bot con tecniche di elusione (quali web scraping, superamento dei reCAPTCHA, generazione di cookie, ecc.) ed era disposto a pagare 15 000 dollari USA (circa 12 750 euro) per il candidato giusto.[4]

_Il Silexbot distruttore

Nel giugno 2019 un ricercatore nel campo della sicurezza[17] ha analizzato un campione di nuovo bot sviluppato per alterare le funzionalità dei dispositivi IoT vulnerabili. In altre parole, questo bot era stato progettato per sfruttare le credenziali conosciute/predefinite dei dispositivi IoT per effettuare il login e quindi distruggere il dispositivo cancellando le configurazioni di rete e aggiungendo una regola in IPtables per eliminare tutte le connessioni. Oltre alle capacità tecniche, un aspetto interessante è stato la nota lasciata sul campione di malware. L'attore della minaccia si scusava per il gesto, giustificandolo come tentativo di prevenire lo sfruttamento di massa di dispositivi IoT vulnerabili per costruire botnet a scopi dolosi.

_Echobot e il suo vettore di minacce in crescita

Nel giugno 2019 un ricercatore nel campo della sicurezza ha individuato una versione aggiornata di Echobot. Nella sua analisi il ricercatore ha osservato un campione compilato in x86 che portava a vettori di attacco utilizzati da questa variante di Mirai in 26 diversi incidenti.[10] In agosto un altro ricercatore ha scoperto un incremento di Echobot, che sfruttava 50 diverse vulnerabilità tra cui la «command injection over HTTP» (CPAI-2016-0658).[25,26] Nel dicembre 2019 un altro team ha rilevato una versione potenziata di Echobot, comprendente 71 exploit. I nuovi exploit aggiunti prendevano di mira vulnerabilità vecchie e nuove e avevano una capacità significativamente maggiore di puntare ai dispositivi ICS (sistemi di controllo industriale). Questo includeva aziende e dispositivi come Mitsubishi, controlli di distribuzione delle applicazioni Citrix NetScaler, firewall per applicazioni web Barracuda e strumenti di amministrazione degli endpoint.[27]

_Necurs in declino, mentre Emotet riprende a salire

Nel corso del gennaio 2019 si è osservata la trasformazione di Necurs in campagna di spam di tipo amatoriale, il che ha portato i ricercatori a ipotizzare una significativa diminuzione delle competenze degli attori malintenzionati che si nascondono dietro tale botnet.[20] Viceversa, l'attività di Emotet è aumentata sostanzialmente dal settembre 2019 e ha continuato a crescere verso la fine del 2019, installando file binari compilati unici che rappresentano vettori di consegna e meccanismi di comunicazione persistenti.[7] Un'analisi ha rivelato un netto aumento della distribuzione di Emotet via e-mail.[22]

Tendenze

_Retadup, la botnet dietro il mining di Monero, è caduta

Retadup è stata attiva principalmente come worm per il mining di Monero, che ha sviluppato capacità polimorfiche[23] e aveva infettato le macchine Windows in America latina. Questo bot aveva capacità che andavano dal mining alla distribuzione di codice personalizzato ed eseguiva il download di file sulle macchine delle vittime (si è osservata anche la distribuzione di ransomware STOP[24]). Un ricercatore della sicurezza ha iniziato a monitorare l'attività di Retadup nel marzo 2019 e ha notato che il protocollo C2 era stato progettato in modo semplice. Il team ha individuato un difetto del protocollo che gli ha permesso di rimuovere le infezioni dalla vittima prendendo il controllo del server C2. È stato scoperto che l'infrastruttura per questa attività malevola si trovava prevalentemente in Francia. La botnet è stata abbattuta con la collaborazione della Gendarmeria nazionale francese e circa 850 000 computer sono stati disinfettati.

_Mirai è morto, lunga vita a Mirai

Potrebbe essere a causa della mancanza di competenze e funzioni nel codice originale che Mirai e le sue varianti dominano tuttora tra le famiglie di botnet, e più di 20 000 campioni unici sono stati osservati ogni mese durante la prima metà del 2019. Queste varianti sfruttano tecniche diverse per compromettere gli IoT, dalla forzatura bruta di password predefinite a codifica fissa (hard-coded) agli exploit.[6] Vi è inoltre un'ampia eterogeneità di architetture di sistema che, secondo due ricercatori della sicurezza, sono state bersaglio di queste varianti. Ulteriori statistiche sull'attività di Emotet sono riportate nella figura 1.[7,18]

_La botnet P2P Roboto

L'attività di Roboto è stata osservata per la prima volta nell'agosto del 2019, da un team di ricerca sulla sicurezza, come programma botnet P2P. Il primo campione rilevato era un file ELF sospetto. In ottobre il team di ricerca ha identificato un altro campione (file ELF) che si è rivelato essere il downloader del campione precedente. A un'ulteriore analisi il team di ricerca ha scoperto che la botnet Roboto è in grado di supportare sette funzioni: reverse shell, autodisattivazione, raccolta di informazioni sul processo e sulla rete, raccolta di informazioni sul bot, esecuzione di file con URL specifici, attacchi DDoS ed esecuzione di attacchi al sistema. È interessante notare che, secondo il ricercatore, un attacco DDoS non è il suo caso d'uso principale. A differenza di altre botnet, questo bot si è diffuso sfruttando la vulnerabilità Webmin RCE (CVE-2019-1507[28]).[11]

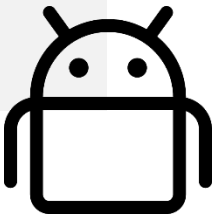
_Mozi, un'altra botnet basata su DHT

Mozi, che prende il nome dal suo file di propagazione, è stato identificato come nuovissima botnet basata su DHT da un ricercatore della sicurezza nel settembre 2019. Un'analisi iniziale del campione eseguita da un altro ricercatore[38] lo ha identificato come Gafgyt, ciò a causa del fatto che il campione ha parzialmente riutilizzato il codice di Gafgyt. Questa botnet si diffonde utilizzando una manciata di exploit e sfruttando password deboli per telnet. L'analisi delle sue funzionalità ha rivelato che potrebbe essere in grado di lanciare attacchi DDoS, raccogliere informazioni, eseguire e aggiornare il campione/payload utilizzando un URL specificato ed eseguire comandi[29, 30]

Statistiche sull'attività di Emotet

Risultato	Statistica
Numero totale di ASN rilevati:	5 430
Numero totale di IP unici rilevati:	120 764
Paesi totali partecipanti:	193
E-mail totali inviate:	10 935 346
URL di distribuzione totali:	4 726
RCPT distinti presi di mira:	8 052 961

Figura 1. Fonte: Spamhaus[5]



«I progressi tecnologici nel calcolo distribuito e nell'automazione hanno offerto ad attori malintenzionati l'opportunità di esplorare nuove tecniche e di migliorare strumenti e metodi di attacco».

in ETL 2020

Risultati

_Statistiche e altri dati di rilievo

Secondo un ricercatore nel campo della sicurezza, **7,7 milioni di dispositivi IoT si collegano a Internet ogni giorno** e si stima che solo 1 su 20 sia protetto da un firewall o strumento di sicurezza di rete analogo.[6] Questa stima rivela che **i dispositivi IoT sono ancora vulnerabili e pronti a essere sfruttati** dalle minacce alla cibersicurezza come Mirai.

- Nella prima metà del 2019 l'attività delle botnet e dei server C2 che le ospitano è cresciuta in modo sostanziale.[32] Questo aumento ha rappresentato il 7% di tutte le rilevazioni di botnet e l'1,8% dei C2 a livello mondiale. I servizi finanziari e i loro clienti sono stati il settore più spesso preso di mira.
- La Thailandia è risultata il primo paese riguardo all'hosting di server C2, al secondo posto figura la Malesia, seguita da Filippine, Singapore e Indonesia.
- Sulla base delle ricerche dell'Interpol, la botnet Andromeda è risultata dominante in termini di rilevamento, anche se è stata smantellata nel 2017.[33] Conficker[34] si è posizionato secondo, seguito da Necurs[35], Sality[36] e Gozi[37].

Nel corso del 2019 il numero di varianti Mirai rilevate è aumentato di oltre il 57% rispetto al 2018, come illustrato nella figura 2.

Sebbene le varianti di Mirai siano note per utilizzare tentativi di forza bruta prevalentemente per compromettere i dispositivi IoT, nel corso del 2019 si è osservato un aumento sia dei tentativi di forza bruta (51%) sia dello sfruttamento del web (87%).

Calcolo dei campioni di Mirai

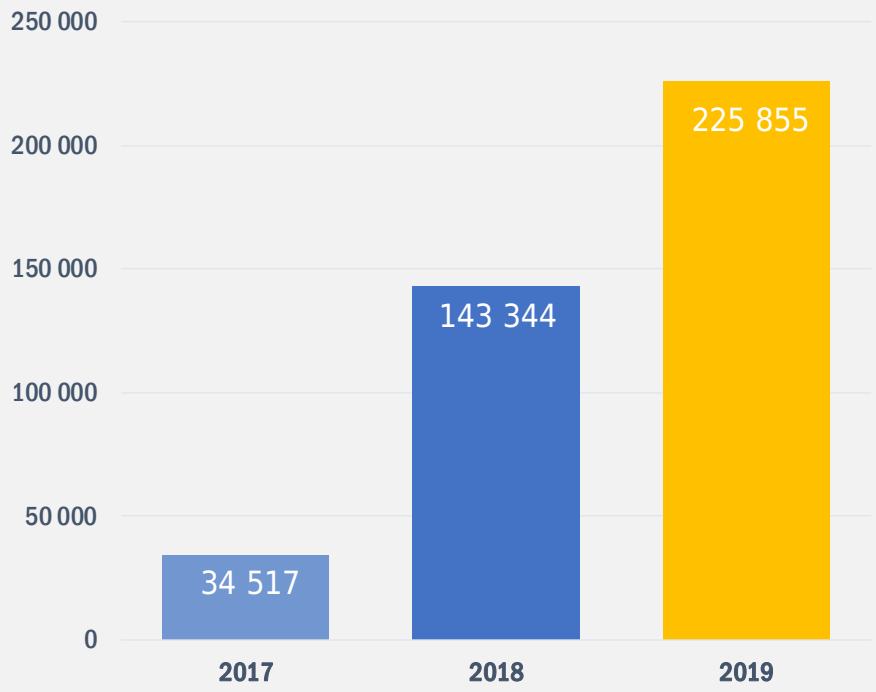


Figura 2 - Fonte: NETSCOUT[7]

Risultati

_Statistiche e altri dati di rilievo

- Nel corso del 2019 un ricercatore della sicurezza ha osservato quasi 300 000 notifiche in più di traffico di botnet di Emotet e oltre 100 000 segnalazioni di vittime in più rispetto allo stesso periodo del 2018. Sulla base di un confronto tra il secondo semestre del 2018 e quello del 2019, i ricercatori ritengono che vi sia stato un aumento del 913% del numero di campioni di Emotet.[7,22]
- Si è osservato un aumento dell'attività delle botnet P2P da quando Roboto e Mozi sono diventati attivi.[8]
- Le botnet basate su Linux sono state responsabili di quasi il 97,4% degli attacchi.[8]
- La quota più elevata di botnet è stata registrata negli Stati Uniti (58,33%) nel quarto trimestre del 2019. Pur con un aumento rispetto al 3 ° trimestre 2019 (47,55%), il numero totale di server C2 si è quasi dimezzato. Il Regno Unito è balzato da quarto al secondo posto con il 14,29%, mentre la Cina ha mantenuto la stessa posizione al 9,52%. Il calo più significativo di server C2 registrati è stato osservato nei Paesi Bassi (dal 45% a ~1%). Per maggiori informazioni sulla distribuzione dei server C2 di botnet per paese, si rimanda alla figura 3.[8]
- Nel 2019 LokiBot è rimasto in cima alla lista dei bot attivi nel furto delle credenziali, con un aumento del 74% del numero di attività di C2 rispetto al 2018. AZORult si trovava in seconda posizione subito dopo LokiBot.[39]
- Nel corso del 2019 erano attivi 17 602 server C2 di botnet, con un aumento del 71,5% rispetto al 2018.[39]

Distribuzione dei server C&C di botnet per paese

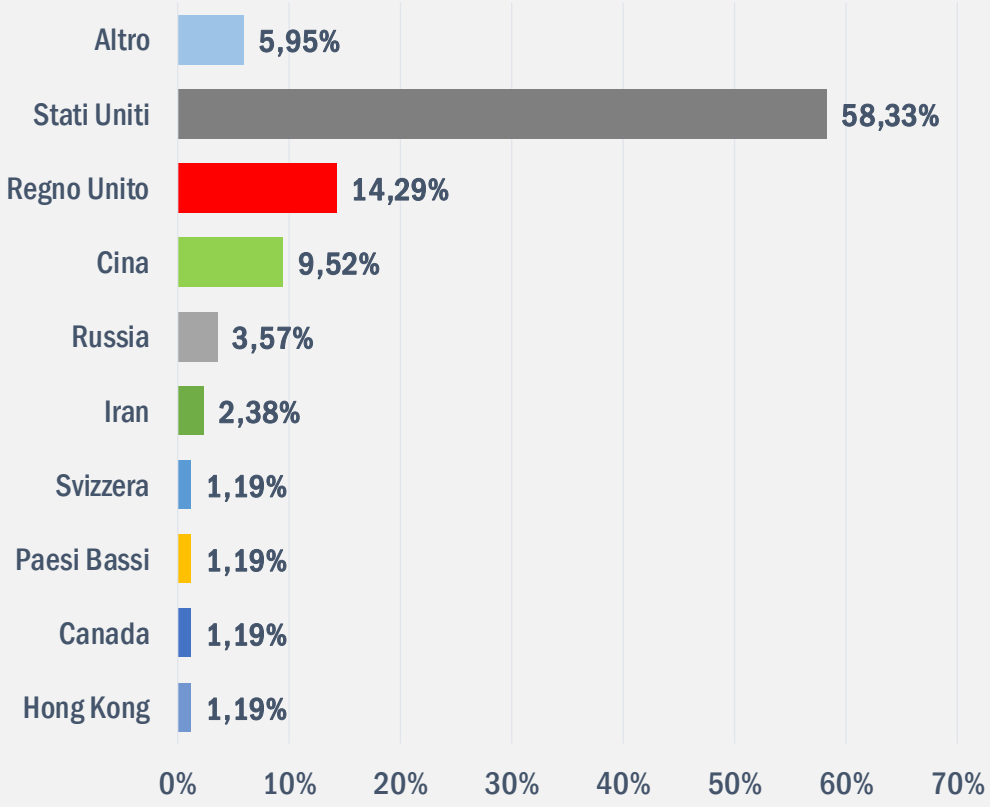


Figura 3 - Fonte: Kapersky[8]

Vettori di attacco

_ Gli attacchi di botnet

Secondo un ricercatore della sicurezza, nel 2019 quasi il 60% dell'attività delle nuove botnet rivali era associato al **furto di credenziali**. Come accennato in precedenza, LokiBot è il più attivo in questo campo. Oltre all'attività di furto di credenziali, **l'e-banking e le frodi finanziarie** sono altre aree in cui si osserva una vasta presenza di botnet. Emotet e TrickBot sono gli esempi principali di questa attività, con un modello aggiornato che interessa non solo le frodi legate all'e-banking ma anche il pay-per-install (PPI).[9]

Inoltre, i **trojan di accesso remoto (Remote Access Trojan, RAT)** sono stati tra gli strumenti più utilizzati nelle attività dei C2 di botnet. Nel corso del 2018 la maggior parte di queste attività è stata associata ad Adwind, ma nel 2019 la sua attività si è ridotta ed è stata sostituita da NanoCore.[5]

Nel 2019 **sono stati adottati vettori di attacco specifici**. Le botnet utilizzano diversi vettori di attacco per raggiungere i loro obiettivi. Macchine infette o reti zombie vengono create sfruttando le vulnerabilità comuni con tecniche di forza bruta e altre tecniche di infezione comuni.[10,11,12] Successivamente il botmaster è in grado di fornire una piattaforma per diversi attacchi, tra cui la diffusa campagna di spamming e malware, furto e riutilizzo delle credenziali, cryptomining e DDoS.

Un altro esempio di vettore utilizzato in un attacco di botnet è la **«tripla minaccia»**. Questa tecnica prevede che l'organizzazione bersaglio venga inizialmente infettata dal malware Emotet↗. Tale malware veicola poi il trojan TrickBot, che prende di mira ed esplora le informazioni sensibili. Se si trovano informazioni e l'ambiente/rete bersaglio figura nell'elenco dell'aggressore, viene veicolato il ransomware Ryuk.[13]

Numero di server C2 di una botnet osservati tra il 2014 e il 2019

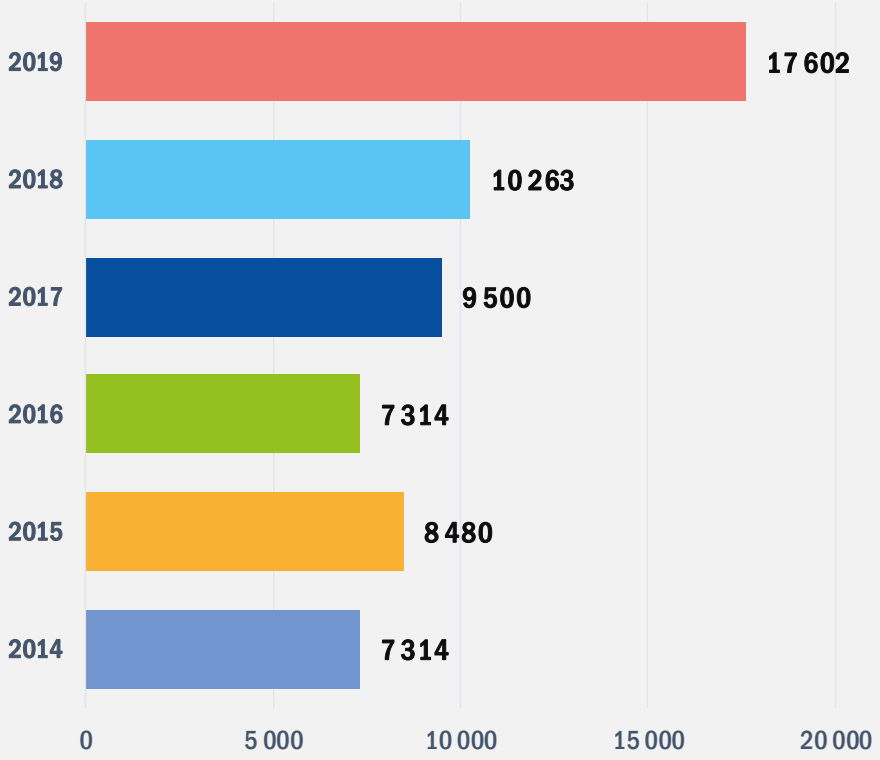


Figura 4 - Fonte: Spamhaus[5]

Mitigazione

_ Azioni proposte

Un aspetto fondamentale di una difesa solida è il concetto di conoscenza dell'ambiente. Ciò aiuta a identificare le attività dannose all'interno del traffico sulla base della possibile linea di riferimento, o baseline (cioè i rilevamenti comportamentali),[14] misurata mediante uno strumento di monitoraggio del traffico.[4] Dato che un consistente traffico botnet è associato all'attività DDoS, si applicano anche tecniche di mitigazione di tale minaccia.

- Implementare feed BGP (Border Gateway Protocol) con la capacità di cercare dTLD (domini di primo livello decentralizzati) al fine di bloccare le connessioni agli indirizzi IP correlati all'attività del C2 di botnet.[8]
- Comprendere e classificare le vulnerabilità e attuare una solida pratica di installazione di patch e aggiornamenti.[15,16]
- Limitare o bloccare i pool di mining di criptovalute e monitorare l'ambiente per gli utenti richiesti.[5]
- Implementare funzionalità basate su sfide per i siti web richiesti al fine di controllare l'origine del traffico (ossia i reCAPTCHA).[16]
- Attuare politiche di password e autenticazione forti (2FA) su server o infrastrutture rivolte al pubblico, per evitare di subire attacchi che sfruttano password/autenticazione deboli.[5]
- Implementare e configurare firewall di rete e delle applicazioni.

«La complessità delle competenze in materia di minacce è aumentata nel 2019, con molti avversari che utilizzano exploit, furto di credenziali e attacchi a più livelli».

in ETL 2020

Riferimenti bibliografici

1. «Peer-to-peer (P2P).” Malwarebytes Labs https://blog.malwarebytes.com/glossary/peer-to-peer/
2. Monnappa K A. «Learning Malware Analysis.» Giugno 2018. O’reilly. https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/17a1735d-9583-4d86-9d1e-8b2735af5168.xhtml
3. «ASEAN Cyberthreat Assessment 2020.» 17 febbraio 2020. Interpol https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-key-cyberthreats-in-Southeast-Asia
4. «State of The Internet Security - DDoS and Application Attacks Report: Volume 5, Issue 1.» 2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf
5. «Spamhaus Botnet Threat Report 2019.» 28 gennaio 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019
6. «NETSCOUT Threat Intelligence Report: Powered by ATLAS - Findings from H1 2019.» 2019.
7. «NETSCOUT Threat Intelligence Report - With key findings from the 15th Annual Worldwide Infrastructure Security Report (WISR) - Findings from H2 2019.» 2019. NETSCOUT. https://www.netscout.com/threatreport
8. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. «DDoS attacks in Q4 2019.» 13 febbraio 2020. Kaspersky. https://securelist.com/ddos-report-q4-2019/96154/
9. Alina Dettmer. «What is Pay Per Install.?» 26 ottobre 2017. Aye Studios. https://www.ayetstudios.com/blog/mobile-advertising/mobile-campaign-types/pay-per-install
10. Larry Cashdollar. «Latest Echobot: 26 Infection Vectors.» 13 giugno 2019. Akamai. https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html
11. «The awaiting Roboto Botnet.» 20 novembre 2019. Netlab. https://blog.netlab.360.com/the-awaiting-roboto-botnet-en/
12. Asher Davila. «Home & Small Office Wireless Routers Exploited to Attack Gaming Servers.» 31 ottobre 2019. Paloalto. https://unit42.paloaltonetworks.com/home-small-office-wireless-routers-exploited-to-attack-gaming-servers/
13. «Triple Threat: Emotet deploys Trickbot to steal data & spread Ryuk.» 2 aprile 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware
14. «Bots.» Imperva. https://www.imperva.com/learn/application-security/what-are-bots/
15. Rebecca Carter. «Bot Mitigation Best Practices.» 19 ottobre 2018. DYN. https://dyn.com/blog/bot-mitigation-best-practices/
16. «What is a Botnet?» Veracode. https://www.veracode.com/security/botnet
17. «SIRT Advisory: Silexbot bricking systems with known default login credentials». 26 giugno 2019. Akamai.
18. «Mirai Botnet Continues to Plague IoT Space». 10 settembre 2019. Reversing Labs. https://blog.reversinglabs.com/blog/mirai-botnet-continues-to-plague-iot-space
19. The Shadowserver Foundation. https://www.shadowserver.org/
20. «As Necurs Botnet Falls from Grace, Emotet Rises» 27 gennaio 2020. Threat Post. https://threatpost.com/as-necurs-botnet-falls-from-grace-emotet-rises/152236/

21. «Mirai malware, attacks Home Routers». 14 dicembre 2016. ENISA. https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

22. «Estimating Emotet's size and reach». 12 dicembre 2019. SPAMHAUS. https://www.spamhaus.org/news/article/791/estimating-emotets-size-%20-and-reach

23. «Monero-Mining RETADUP Worm Goes Polymorphic, Gets an AutoHotKey Variant». 23 aprile 2018. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/

24. «Meet Stop Ransomware: The Most Active Ransomware Nobody Talks About». 20 settembre 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/meet-stop-ransomware-the-most-active-ransomware-nobody-talks-about/

25. «Command Injection Over HTTP». 26 luglio 2016. Check Point. https://www.checkpoint.com/defense/advisories/public/2016/cpai-2016-0658.html/

26. «August 2019's Most Wanted Malware: Echobot Launches Widespread Attack Against IoT Devices». Agosto 2019. Check Point. https://blog.checkpoint.com/2019/09/12/august-2019s-most-wanted-malware-echobot-launches-widespread-attack-against-iot-devices/

27. «Echobot Malware Now up to 71 Exploits, Targeting SCADA». 18 dicembre 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada

28. «CVE-2019-15107 Detail». NIST. https://nvd.nist.gov/vuln/detail/CVE-2019-15107

29. «What is a distributed hash table?». EDPresso. https://www.educative.io/edpresso/what-is-a-distributed-hash-table

30. «A Look into the Gafgyt Botnet Trends from the Communication Traffic Log». 23 luglio 2019. https://nsfocusglobal.com/look-gafgyt-botnet-trends-communication-traffic-log/

32. «ASEAN Cyberthreat Assessment 2020, Key Insights From The ASEAN Cybercrime Operations Desk» Interpol, 2020

33. «International team takes down virus-spewing Andromeda botnet». 5 dicembre 2017. The Register. https://www.theregister.com/2017/12/05/international_team_takes_down_virusspewing_andromeda_botnet/

34. «The odd, 8-year legacy of the Conficker worm». 21 novembre 2016. WeLiveSecurity. https://www.welivesecurity.com/2016/11/21/odd-8-year-legacy-conficker-worm/

35. «The Necurs Botnet: A Pandora's Box of Malicious Spam». 24 aprile 2017. https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/

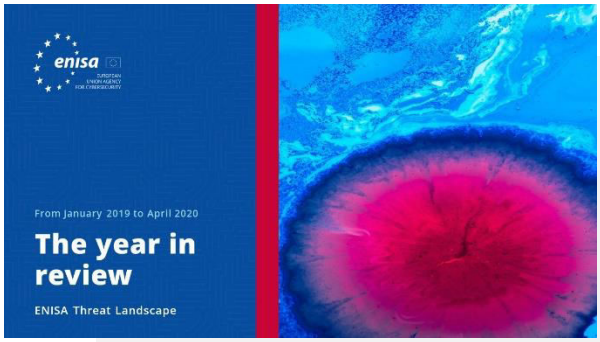
36. «WhitePaper: Sality: Story of a Peer to-Peer Viral Network». 10 giugno 2011. Broadcom.

37. «Botnet C&C: Gozi». FortiGuard Labs. https://fortiguard.com/encyclopedia/botnet/7630489

38. Virustototal. https://www.virustotal.com

39. «Spamhaus Botnet Threat Report 2019» 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

Correlati



Relazione sul panorama delle minacce dell'ENISA **L'anno in rassegna**

Una sintesi delle tendenze nella cibersicurezza per il periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Elenco delle prime 15 minacce

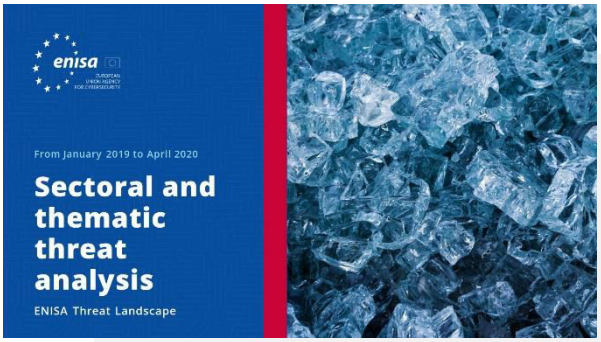
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Argomenti di ricerca

Raccomandazioni su argomenti di ricerca di vari quadranti nella cibersicurezza e nell'intelligence sulle minacce informatiche.

LEGGI LA RELAZIONE



Relazione sul panorama delle minacce dell'ENISA **Analisi delle minacce settoriali e tematiche**

Analisi contestualizzata delle minacce tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Tendenze emergenti**

Principali tendenze nella cibersicurezza osservate tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Quadro generale dell'intelligence sulle minacce informatiche

Situazione attuale dell'intelligence sulle minacce informatiche nell'UE.

LEGGI LA RELAZIONE

Informazioni

_ L'agenzia

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza contribuisce alla politica dell'UE in questo campo, aumenta l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche di domani. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sulle sue attività sono disponibili al seguente indirizzo: www.enisa.europa.eu.

Autori

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) e *tutti i componenti del gruppo di portatori di interessi sulla CTI dell'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) e Thomas Hemker.

Redattori

Marco Barros Lourenço (ENISA) e Louis Marinos (ENISA).

Contatti

Per informazioni sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.
Per richieste dei media sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.

Saremmo lieti di ricevere il vostro feedback su questa relazione.
Dedicate un momento alla compilazione del questionario. Per accedere al modulo, fare clic qui.

Avvertenza legale

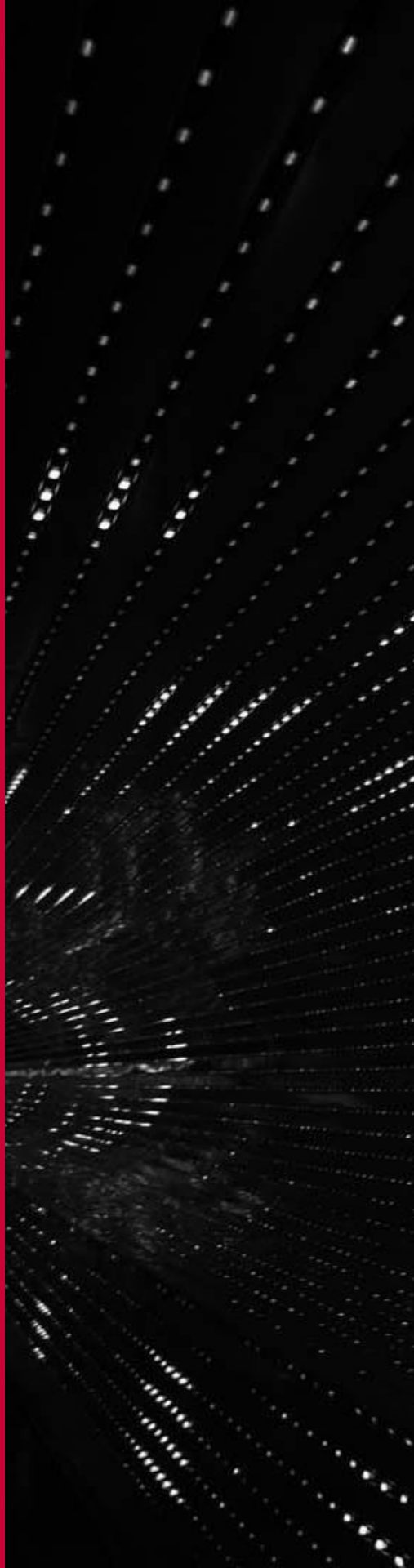
Si rammenta che, salvo diversamente indicato, la presente pubblicazione riflette l'opinione e l'interpretazione dell'ENISA. La presente pubblicazione non deve intendersi come un'azione legale intrapresa dall'ENISA o da suoi organi, a meno che non venga adottata ai sensi del regolamento (UE) N. 526/2013. La presente pubblicazione non rappresenta necessariamente lo stato dell'arte e l'ENISA si riserva il diritto di aggiornarla di volta in volta.

Secondo necessità, sono state citate anche fonti di terze parti. L'ENISA non è responsabile del contenuto delle fonti esterne, quali i siti web esterni riportati nella presente pubblicazione.

La presente pubblicazione è unicamente a scopo informativo. Deve essere accessibile gratuitamente. L'ENISA, o chiunque agisca in suo nome, declina ogni responsabilità per l'uso che può essere fatto delle informazioni di cui alla presente pubblicazione.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu