enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

Malware

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Il malware è un tipo comune di attacco informatico sotto forma di software malevolo. Le famiglie di malware comprendono cryptominer, virus, ransomware, worm e spyware. Gli obiettivi tipici sono il furto di informazioni o di identità, lo spionaggio e l'interruzione dei servizi.[1]

Nel corso del 2019 i cryptominer sono stati una delle famiglie di malware più diffuse nel panorama delle minacce,[2] con conseguenti elevati costi informatici, aumento del consumo di elettricità e riduzione della produttività dei dipendenti.[3] Nel 2019 il ransomware ha registrato un leggero aumento rispetto al 2018, pur rimanendo in fondo alla classifica delle tipologie di malware.[2]

I protocolli web e di posta elettronica sono stati i vettori di attacco iniziali più comunemente utilizzati per diffondere il malware. Tuttavia, attraverso tecniche di forza bruta o lo sfruttamento delle vulnerabilità dei sistemi, alcune famiglie di malware sono riuscite a diffondersi ulteriormente all'interno di una rete. Sebbene i rilevamenti globali degli attacchi siano rimasti ai livelli dell'anno precedente, si è osservato un chiaro spostamento degli obiettivi, dai consumatori verso le imprese.[4]

Risultati

400 000_ **rilevamenti di spyware e adware preinstallati su dispositivi mobili**[4]

13%_ **di aumento dei malware per Windows rilevati negli endpoint aziendali a livello globale**[4]

Il 71%_ **delle organizzazioni ha subito attività di malware con diffusione da un dipendente all'altro**[47]

Il 46,5%_ **di tutto il malware nei messaggi e-mail è stato rilevato nei file in formato .docx**[24]

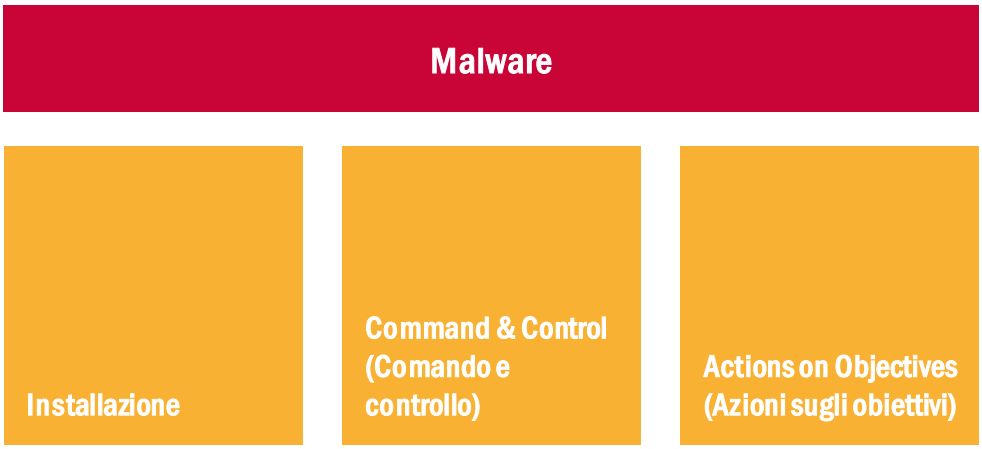
50%_ **di aumento del malware progettato per il furto di dati personali o stalkerware**[15]

Il 67%_ **del malware è stato veicolato attraverso connessioni HTTPS crittografate**[48]

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

Tende

_ Tipi di malware prevalenti

Emotet è stato il ceppo di malware più diffuso nel 2019 ed è in evoluzione nel 2020. Emotet è stato scoperto inizialmente nel 2014 come trojan bancario. Da allora, è stato aggiornato con funzionalità di comando e controllo (C2), meccanismi di elusione aggiuntivi, come la capacità di rilevare se sta girando in un ambiente sandbox e di veicolare payload pericolosi, come Trickbot e Ryuk.[7] La figura presenta la classifica dei malware bancari rilevati nel 2019.

Durante il periodo in esame, Emotet si è evoluto in una botnet[2], ha incrementato la sua attività[8] e ha avviato nuove campagne localizzate di spam con funzionalità di spear phishing finalizzate all'installazione di ransomware o al furto di informazioni.[5] Nel corso del 2019 i rilevamenti di Emotet sono aumentati del 73% rispetto all'anno precedente e gli attacchi hanno preso di mira principalmente gli endpoint aziendali negli Stati Uniti e nel Regno Unito, come illustrato nella figura seguente.[4]

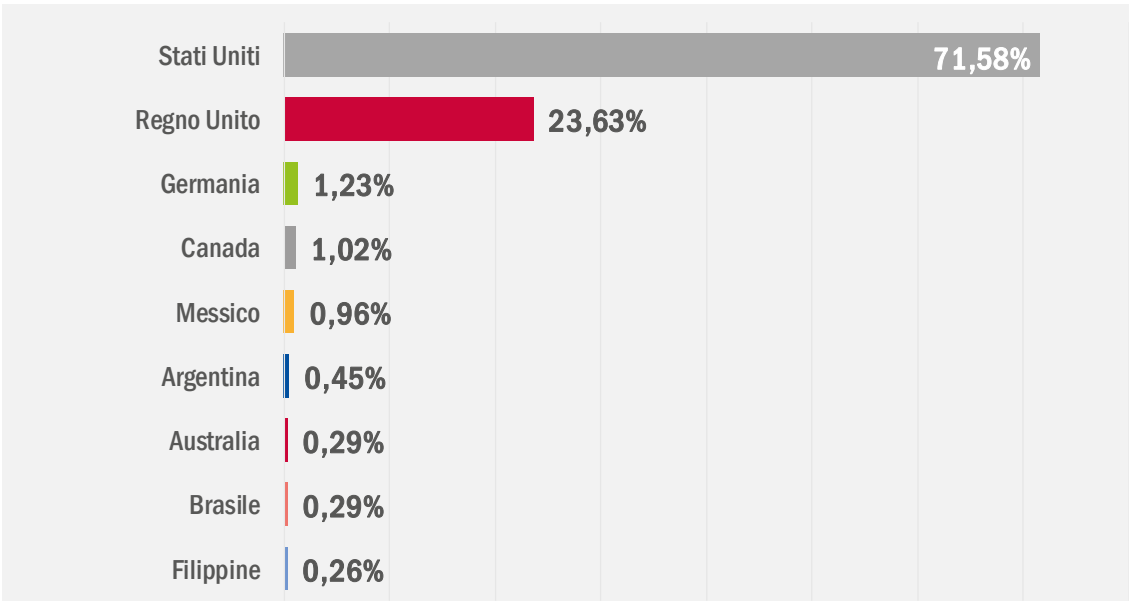


Figura 1. Rilevamenti globali di Emotet nel 2019 per paese. Fonte: MalwareBytes[4]

_Spostamento verso obiettivi aziendali

Sebbene i rilevamenti di malware a livello globale siano rimasti agli stessi livelli del 2018[4,9], si è osservato un aumento del 13% del malware diretto alle imprese, con i settori dei servizi, dell'istruzione e della vendita al dettaglio tra quelli maggiormente colpiti.[4] Si stima che oltre un terzo degli attacchi di malware bancari nel 2019 abbia preso di mira utenti aziendali, con l'intenzione di compromettere le risorse finanziarie dell'azienda.[10] I primi cinque ceppi di malware[4] mirati alle imprese sono stati Trojan.Emotet, Adware.InstallCore, HackTool.WinActivator, Riskware.BitCoinMiner e Virus.Renamer. Nel 2019 sono aumentati gli attacchi ransomware diretti al settore pubblico, per via della capacità di quest'ultimo di pagare riscatti più elevati.[11] Dal momento che i criminali informatici puntano a obiettivi di alto valore, i nuovi tipi di malware sono stati concepiti per diffondersi lateralmente all'interno di una rete aziendale, anziché attraverso Internet.[12]

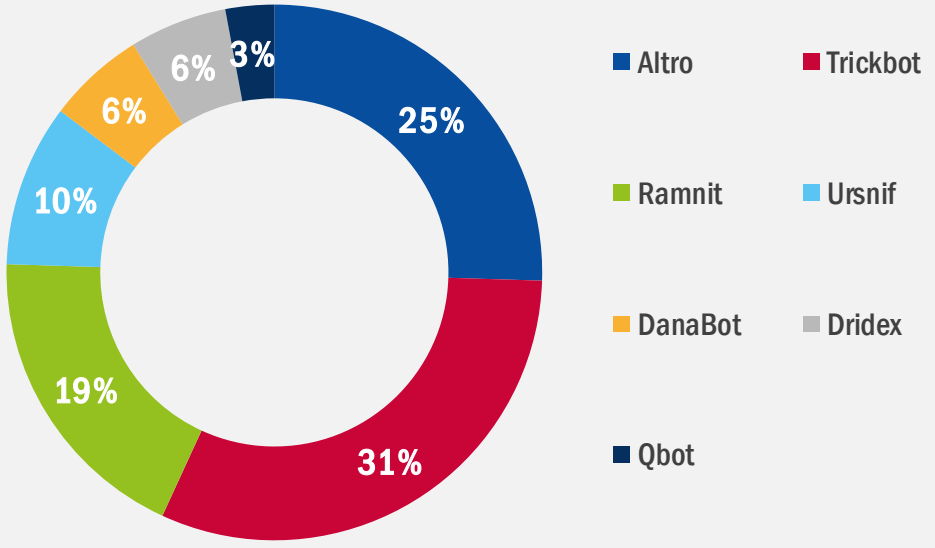


Figura 2. Rilevamenti di malware bancario a livello globale nel 2019. Fonte: CheckPoint[2]

Tendenze

_ Malware-as-a-service (MaaS)

Malware-as-a-service (MaaS) si riferisce a un tipo specifico di malware venduto in forum underground, che fornisce ai clienti (criminali informatici) gli strumenti e l'infrastruttura necessari per attacchi mirati. Il proprietario di MaaS fornisce questo servizio attraverso la consegna di un kit che comprende un loader iniziale, un server di comando e controllo (C2) e una backdoor per assumere il pieno controllo del computer infetto.

Un ricercatore in materia di sicurezza[13] ha di recente individuato quattro tipi di attacchi che utilizzano diversi strumenti del portafoglio Malware-as-a-Service (MaaS) di Golden Chickens (GC), a conferma del rilascio di varianti migliorate con aggiornamenti del codice in tre di questi strumenti.

- **TerraLoader**. Loader polivalente scritto in PureBasic. TerraLoader è uno dei prodotti di punta del portafoglio di servizi MaaS di GC.
- **more_eggs**. Un malware backdoor in grado di effettuare il beaconing su un server C2 fisso e di eseguire ulteriori payload scaricati da una risorsa web esterna. La backdoor è scritta in JavaScript.
- **VenomLNK**. Un file di collegamento di Windows probabilmente generato da una versione più recente del kit di creazione VenomKit.

Impennata del malware bancario su dispositivi mobili

Le applicazioni per dispositivi mobili progettate per rubare dati di pagamento, credenziali e fondi dai conti bancari delle vittime sono aumentate del 50% nella prima metà del 2019.[14] Come da tradizione, gli attori delle minacce hanno utilizzato tecniche di phishing per ottenere le credenziali bancarie, sia visualizzando una pagina falsa che imita la pagina di login della banca, sia introducendo app mobili false che assomigliano a quelle bancarie originali. Nel 2019 i criminali informatici sono diventati tuttavia più creativi, come nel caso di Trojan-Banker.AndroidOS.Gustuff.a, che è riuscito a controllare un'applicazione bancaria legittima attraverso l'uso improprio delle funzioni di accessibilità del sistema operativo, automatizzando così le transazioni dolose.[15] Nuove versioni di malware finanziario per dispositivi mobili si trovavano comunemente in vendita nei forum underground[15] e nuove tecniche di elusione sono state costantemente sviluppate. Una novità degna di nota scoperta nel 2019 è stata la capacità del malware di utilizzare sensori di movimento e di essere attivato solo quando uno smartphone è in movimento, come nel caso del trojan bancario per dispositivi mobili Anubis, nel tentativo di rilevare un ambiente sandbox.[16] I malware bancari più diffusi nel corso del 2019[11] sono stati Asacub (44,4%), Svpeng (22,4%), Agent (19,1%), Faketoken (12%) e Hqwar (3,8%).

_Malware fileless

Il malware fileless, o senza file, non contiene un file eseguibile e può eludere i comuni filtri di sicurezza e le tecniche di whitelisting. Per questo motivo, si tratta di una famiglia di malware che può avere una probabilità di successo fino a dieci volte maggiore rispetto alle altre.[18] Al posto di un file eseguibile, questo tipo di malware prevede che l'aggressore inietti il codice malevolo in un software già installato e affidabile, sia a distanza (ad esempio nel caso della strumentazione gestione Windows o WMI e PowerShell) sia scaricando attivamente file di documenti (ad esempio documenti d'ufficio) contenenti macro dannose.[19] Se l'attacco va a buon fine, il malware può diventare persistente attraverso il registro di sistema, l'utilità di pianificazione integrata o il WMI. Gli attacchi malware fileless sono aumentati del 265% nel primo semestre del 2019.[20] La maggior parte di questi attacchi era basata su script (38%), mentre in altri casi sono avvenuti con l'esecuzione di un attacco in memoria (24%) o l'abuso di strumenti di sistema integrati (20%).[21]

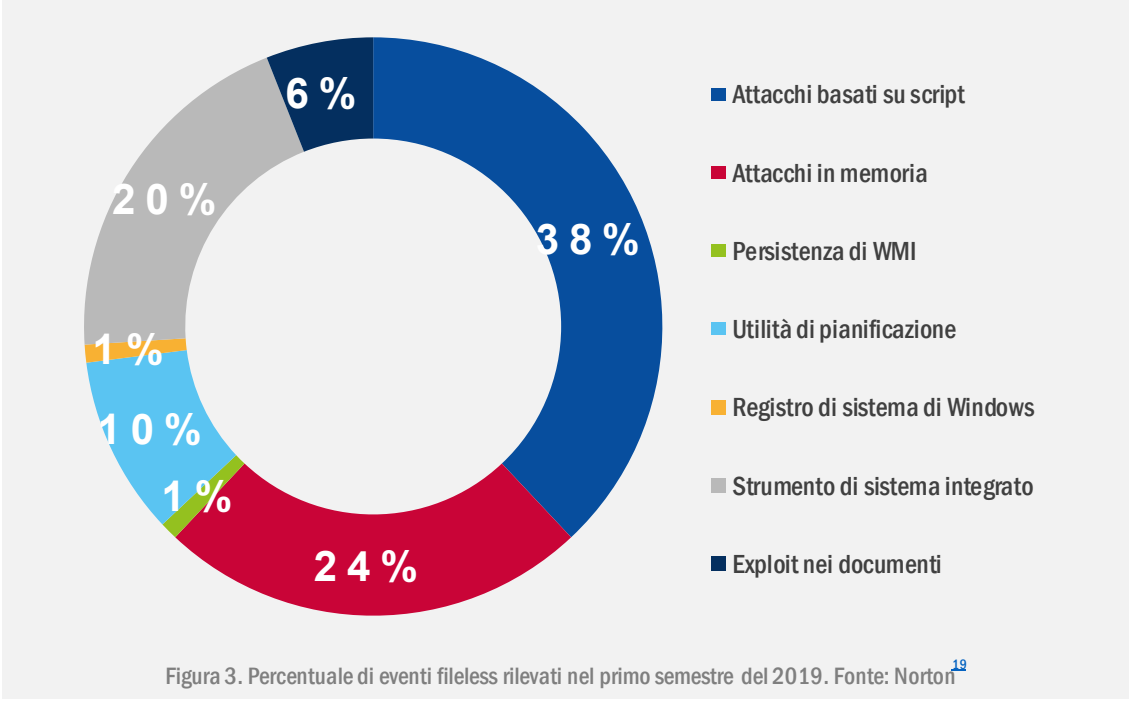


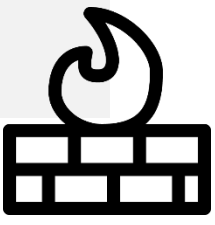
Figura 3. Percentuale di eventi fileless rilevati nel primo semestre del 2019. Fonte: Norton[19]

Come prevenire e difendersi da un attacco fileless?

Il modo più efficace a disposizione delle organizzazioni per difendersi dagli attacchi fileless è mantenere aggiornato il software. Poiché la maggior parte delle infezioni fileless avviene con applicazioni Microsoft, e soprattutto con i file in formato .docx, è particolarmente importante aggiornare costantemente questo software all'ultima versione. Microsoft ha anche aggiornato il suo pacchetto Windows Defender per rilevare attività irregolari mediante l'applicazione PowerShell.

Secondo un ricercatore nel campo della sicurezza[18], la chiave per contrastare con successo una campagna di attacchi fileless è gestire ciascuna delle fasi del ciclo di vita della minaccia con un approccio di difesa integrato e multistrato. In questo approccio è importante indagare le diverse fasi dell'attacco e intraprendere le attività seguenti:

- analizzare e misurare le azioni compiute dall'aggressore;
- identificare le tecniche utilizzate;
- monitorare le attività in PowerShell o altri motori di script;
- accedere a dati aggregati sulle minacce;
- controllare lo stato del sistema preso di mira;
- fermare i processi arbitrari;
- correggere i processi che fanno parte dell'attacco;
- isolare i dispositivi infetti.



_Panorama delle botnet e comando e controllo (C&C)

Rispetto al 2018, il traffico globale di botnet è aumentato complessivamente del 71,5%[2]. Le botnet più spesso osservate sono state Emotet (41%), Trickbot (25%) e DanaBot (5%)[2]. Un chiaro aumento del traffico di botnet è stato osservato in Russia (143%), imputabile soprattutto a procedure di registrazione allentate e a un minore interesse da parte delle forze dell'ordine.[14] Nel corso del 2019, la Russia ha ospitato la maggior parte delle botnet C2, seguita da Stati Uniti, Paesi Bassi, Cina e Francia. Gli algoritmi di generazione di domini (Domain Generation Algorithm) sono stati utilizzati dai criminali informatici per supportare molte comunicazioni C2. Il 50% di queste registrazioni si è verificato nei domini di primo livello (Top-Level Domain, TLD) «.com» e «.net».[15] Nel periodo in esame, tali registrazioni di nomi di dominio sono diminuite del 71%, a favore di altri protocolli di comunicazione come il peer-to-peer (P2P).[13]

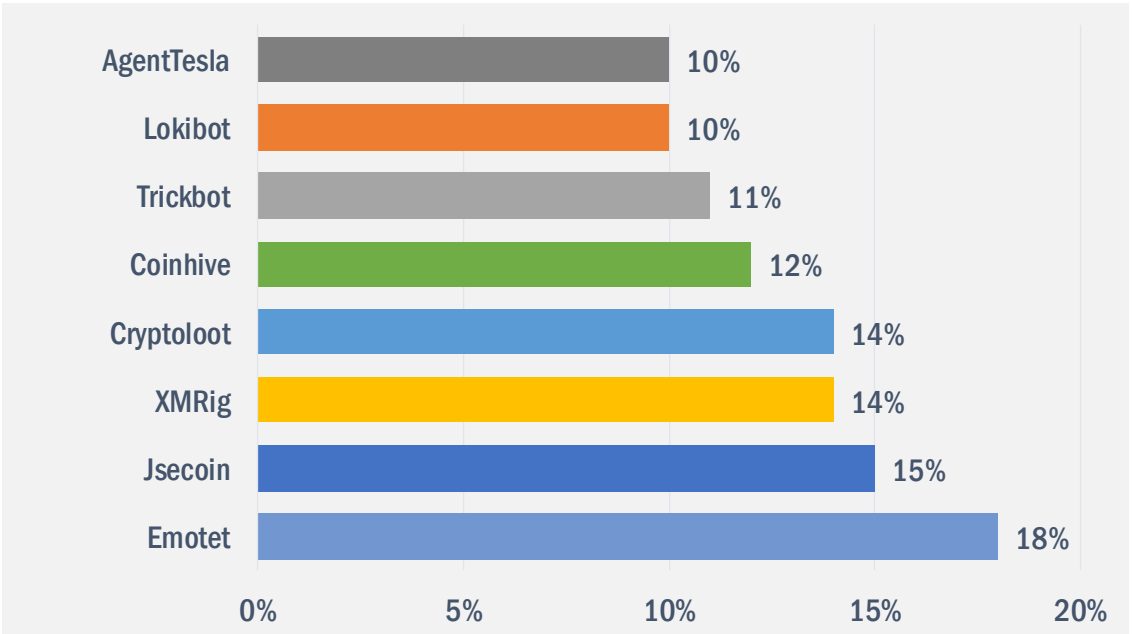


Figura 4. Tipi di malware identificati nel 2019. Fonte: MalwareBytes[4]

_ Come

Secondo uno studio del 2019, il 94% del malware, di ogni tipo, è stato veicolato tramite posta elettronica.[24] Sebbene questo sia considerato un vettore di ingresso, è interessante notare che, se l'attacco va a buon fine, il malware potrebbe scaricare un payload aggiuntivo che si comporta in modo simile a un worm per consentire la diffusione laterale sulla rete (Emotet e Trickbot). Inoltre, dopo la «consegna» iniziale del malware, nella maggior parte dei casi (71%) la diffusione è avvenuta attraverso all'attività dei dipendenti. Ancora una volta, le nuove vulnerabilità nel Remote Desktop Protocol (RDP) hanno attirato l'attenzione, poiché consentono l'esecuzione di codice da remoto (Remote Code Execution, RCE) e sono quindi in grado di propagarsi autonomamente (wormable).[30] Nonostante le nuove vulnerabilità scoperte non siano state sfruttate su vasta scala, è prevedibile che un nuovo worm possa colpire sistemi privi di patch nel prossimo futuro.[31]

_Incidenti

- **Airbus** ha subito una violazione dei dati che ha interessato i dipendenti in Europa.[34,35]
- Un malware per lo skimming delle carte di credito malware installato sul sito web dell'**American Medical Collection Agency** ha causato il furto di 12 milioni di dati personali dei pazienti.[36]
- **LifeLabs,** importante fornitore di servizi diagnostici di laboratorio, è stato vittima di un attacco ransomware che ha portato al furto di 15 milioni di account contenenti risultati di test e numeri delle tessere sanitarie.[37,38]
- In seguito a un attacco ransomware contro la **Città di Pensacola, in Florida,** sono stati resi disponibili online 2 GB di dati, potenzialmente contenenti informazioni sull'identità.[39]
- I dati personali di 2400 **membri delle forze armate di Singapore** potrebbero essere stati divulgati tramite phishing e-mail da malware malevolo.[40]

Mitigazione

Azioni proposte

- Implementare il rilevamento di malware per tutti i canali in entrata/uscita, compresi e-mail, rete, web e sistemi applicativi in tutte le piattaforme pertinenti (ossia server, infrastruttura di rete, personal computer e dispositivi mobili).
- Ispezionare il traffico SSL/TLS consentendo al firewall di decrittare ciò che viene trasmesso da e verso i siti web, le comunicazioni di posta elettronica e le applicazioni per dispositivi mobili.
- Creare interfacce tra le funzioni di rilevamento del malware (ricerca proattiva delle minacce basata sull'intelligence) e la gestione degli incidenti di sicurezza, per determinare capacità di risposta efficienti.
- Utilizzare gli strumenti a disposizione per l'analisi dei malware per condividere le informazioni sui malware e la mitigazione dei malware (ad esempio MISP).[32]
- Elaborare politiche di sicurezza che specifichino i processi da seguire in caso di infezione.
- Comprendere le capacità dei vari strumenti di sicurezza e sviluppare nuove soluzioni di sicurezza. Individuare le lacune e applicare il principio della difesa in profondità.
- Utilizzare il filtraggio della posta (o filtro antispam) per le e-mail malevole e rimuovere gli allegati eseguibili.
- Monitorare regolarmente i risultati dei test antivirus.[30,42]
- Monitoraggio dei log con la soluzione SIEM (Security Incident and Event Management). Fonti di log indicative sono allarmi antivirus, rilevamento e risposta degli endpoint (Endpoint Detection and Response, EDR), log del server proxy, registro eventi di Windows e log di Sysmon,[43] log del sistema di rilevamento delle intrusioni (Intrusion Detection System, IDS)[44], ecc.
- Disattivare o ridurre l'accesso alle funzioni di PowerShell.[45]

«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. «What is Malware». Veracode. https://www.veracode.com/security/malware
2. «Cyber Security Report». 2019. Checkpoint. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf
3. «Beapy: Cryptojacking Worm Hits Enterprises in China» 24 aprile 2019. Broadcom. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china
4. «2020 State of Malware Report». Febbraio 2020. Malware Bytes. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
5. «Evasive Threats, Pervasive Effects» 2019. Trend Micro, Research. https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf
6. «SonicWall Cyber Threat Report». 2020. SonicWall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/
7. «Emotet is back: botnet springs back to life with new spam campaign». 16 settembre 2019. Malwarebytes Labs. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/
8. «Increased Emotet Malware Activity» 22 gennaio 2020. US CERT. https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity
9. «SonicWall Security Metrics» SonicWall. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics
10. «Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection». 16 aprile 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection
11. «Internet organised crime threat assessment» 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf
12. «Narrowed Sights, Bigger Payoffs: Ransomware in 2019» 6 giugno 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019
13. «GOLDEN CHICKENS: Evolution of the MaaS». 20 luglio 2020. QuoIntelligence. https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/
14. «From Supply Chain to Email, Mobile and the Cloud» 25 luglio 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/
15. «Mobile malware evolution 2019». 25 febbraio 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/
16. «Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics». 17 gennaio 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/
17. «Spamhaus Botnet Threat Report 2019.» 28 gennaio 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019
18. «What Is Fileless Malware?». McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html
19. «What is fileless malware and how does it work?» . Norton. https://us.norton.com/internetsecurity-malware-what-is-fileless-malware.html
20. «Trend Micro Report Reveals 265% Growth In Fileless Events». 28 agosto 2019. Trend Micro. https://www.trendmicro.com/en_hk/about/newsroom/press-releases/2019/2019-08-28.html
21. «Understanding Fileless Threats» 29 luglio 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats

22. «SonicWall Sees Dramatic Jump In IoT Malware, Encrypted Threats, Web App Attacks Through Third Quarter». 22 ottobre 2019. SonicWall. https://www.sonicwall.com/news/dramatic-jump-in-iot-malware-encrypted-threats-web-app-attacks-third-quarter/

23. «2020 Vulnerability and Threat Trends». 2020. SKYBOX. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020_VT_Trends-Report-reduced.pdf

24. «Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection». 16 aprile 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection

25. «Internet organised crime threat assessment» 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

26. «Narrowed Sights, Bigger Payoffs: Ransomware in 2019» 6 giugno 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

27. «From Supply Chain to Email, Mobile and the Cloud» 25 luglio 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/

28. «Mobile malware evolution 2019». 25 febbraio 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/

29. «Mobile banking malware surges in 2019». 25 luglio 2019. Computer Weekly. https://www.computerweekly.com/news/252467340/Mobile-banking-malware-surges-in-2019

30. «Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics». 17 gennaio 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

31. «BlueKeep attacks are happening, but it's not a worm». 3 novembre 2019. ZDNet. https://www.zdnet.com/article/bluekeep-attacks-are-happening-but-its-not-a-worm/

32. MISP Projects. http://www.misp-project.org/

33. «PowerShell, fileless malware's great attack vector». 25 febbraio 2019. Panda. https://www.pandasecurity.com/mediacenter/malware/powershell-fileless-malware-attack-vector/

34. «Airbus Statement on Cyber Incident». 30 gennaio 2019. Airbus. https://www.airbus.com/newsroom/press-releases/en/2019/01/airbus-statement-on-cyber-incident.html

35. «Airbus data breach impacts employees in Europe" 30 gennaio 2019. ZDNet. https://www.zdnet.com/article/airbus-data-breach-impacts-employees-in-europe/

36. «Massive Quest Diagnostics data breach impacts 12 million patients». 4 giugno 2019. ZDNet. https://www.zdnet.com/article/massive-quest-diagnostics-data-breach-impacts-12-million-patients/

37. «Hackers crack 15M LifeLabs accounts, obtain lab results and health card numbers». 17 dicembre 2019. Daily Hive. https://dailyhive.com/calgary/lifelabs-hacked-cyber-attack

38. «Why the LifeLabs Hack Likely Is Worse than Most». 18 dicembre 2019. The Tyee. https://thetyee.ca/Analysis/2019/12/18/LifeLabs-Data-Hack/

39. «Personal Information in City of Pensacola Cyberattack». 17 gennaio 2020. Città di Pensacola. https://www.cityofpensacola.com/CivicSend/ViewMessage/Message/100944

40. «Personal data of 2,400 Mindef, SAF staff may have been leaked» 22 dicembre 2019. The Straits Times - Singapore. https://www.straitstimes.com/singapore/personal-data-of-2400-mindef-saf-staff-may-have-been-leaked

Riferimenti bibliografici

41. AVTEST – The Independent IT-Security Institute. https://www.av-test.org/en/

42. «Real world protection tests.» AV Comparatives. https://www.av-comparatives.org/dynamic-tests/

43. «The ThreatHunting Project.» https://www.threathunting.net/data-index

44. Mark Russinovich, Thomas Garnier. «Sysmon v11.10.» 24 giugno 2020. Microsoft. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

45. «Guide to Intrusion Detection and Prevention Systems (IDPS).» Febbraio 2007. CSRC. https://csrc.nist.gov/publications/detail/sp/800-94/final

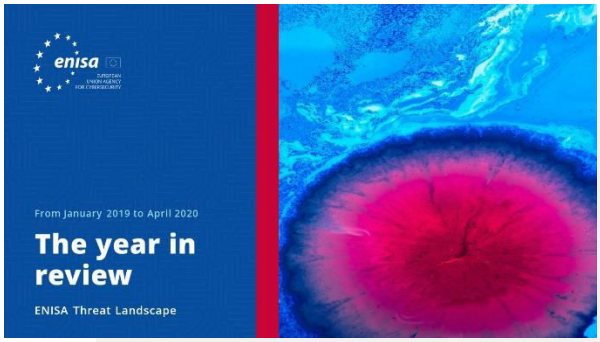
47. «Most malware in Q1 2020 was delivered via encrypted HTTPS connections». 25 giugno 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

48. «Malware statistics and facts for 2020» 29 luglio 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/

«Il panorama delle minacce sta diventando estremamente difficile da mappare. Non solo gli autori degli attacchi sviluppano nuove tecniche per eludere i sistemi di sicurezza, ma le minacce diventano sempre più complesse e precise in attacchi mirati».

in ETL 2020

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

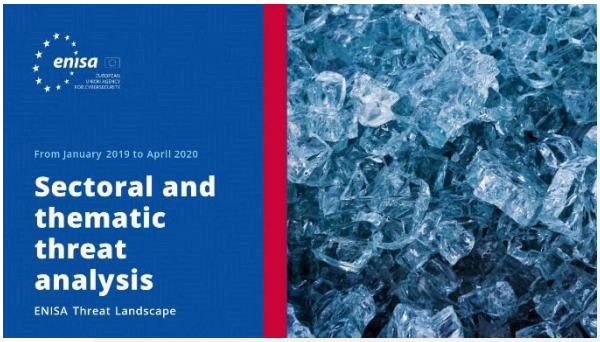
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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