enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

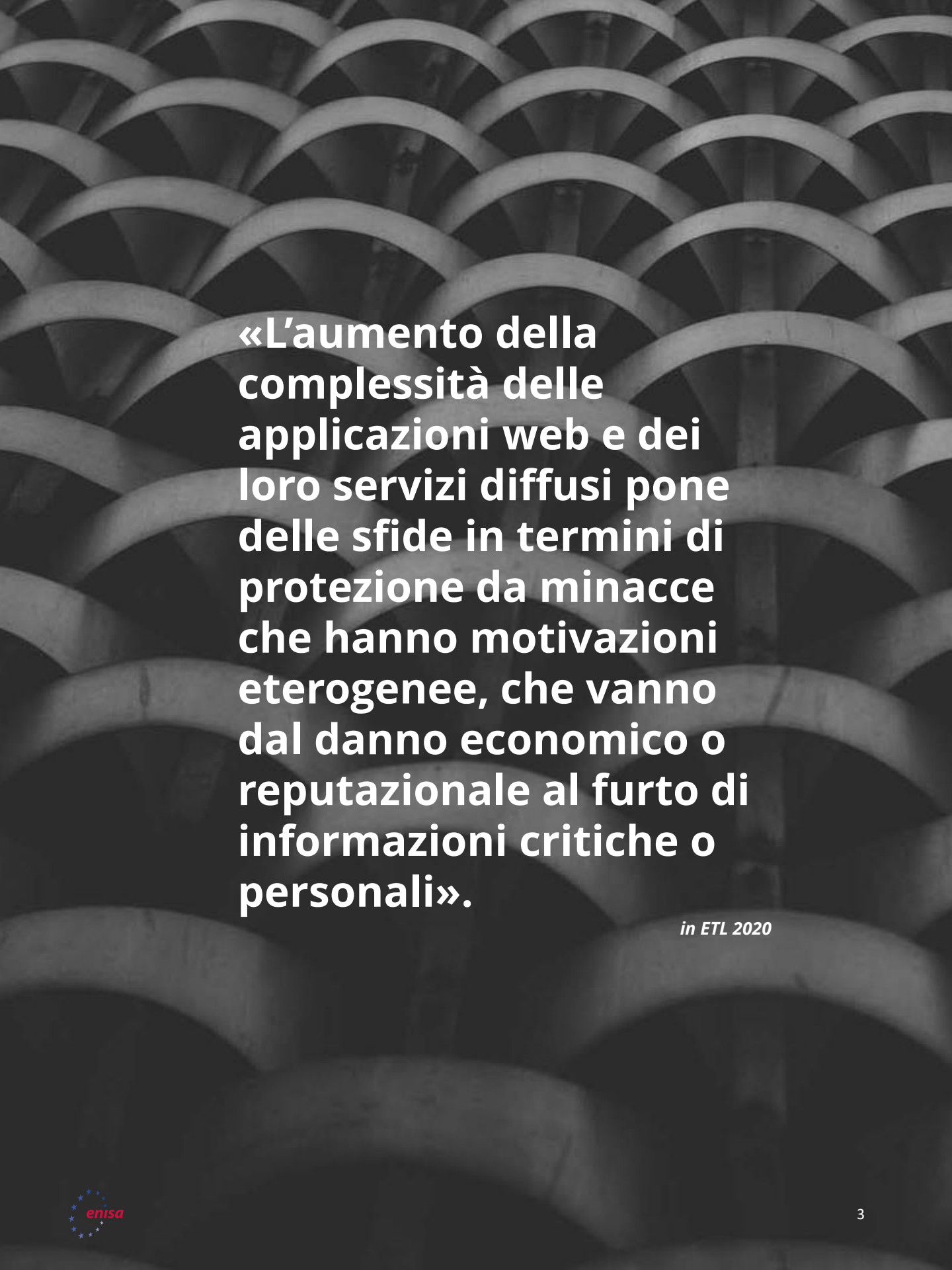
Attacchi basati sul web

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Gli attacchi basati sul web sono un metodo allettante per gli attori delle minacce, che possono ingannare le vittime utilizzando sistemi e servizi web come vettore. Questo copre una vasta superficie di attacco, ad esempio utilizzando URL o script malevoli per indirizzare l'utente o la vittima verso il sito web desiderato oppure scaricando contenuti dannosi (attacchi watering hole[1], attacchi drive-by[2]) e iniettando codice malevolo in un sito web legittimo, ma compromesso, per rubare informazioni (formjacking[3]) a scopo di guadagno, furto di dati o perfino estorsione tramite ransomware.[4] Oltre a questi esempi, gli exploit dei browser e le compromissioni dei sistemi di gestione dei contenuti (Content Management System, CSM) sono stati osservati da diversi team di ricerca come importanti vettori utilizzati da attori malintenzionati.

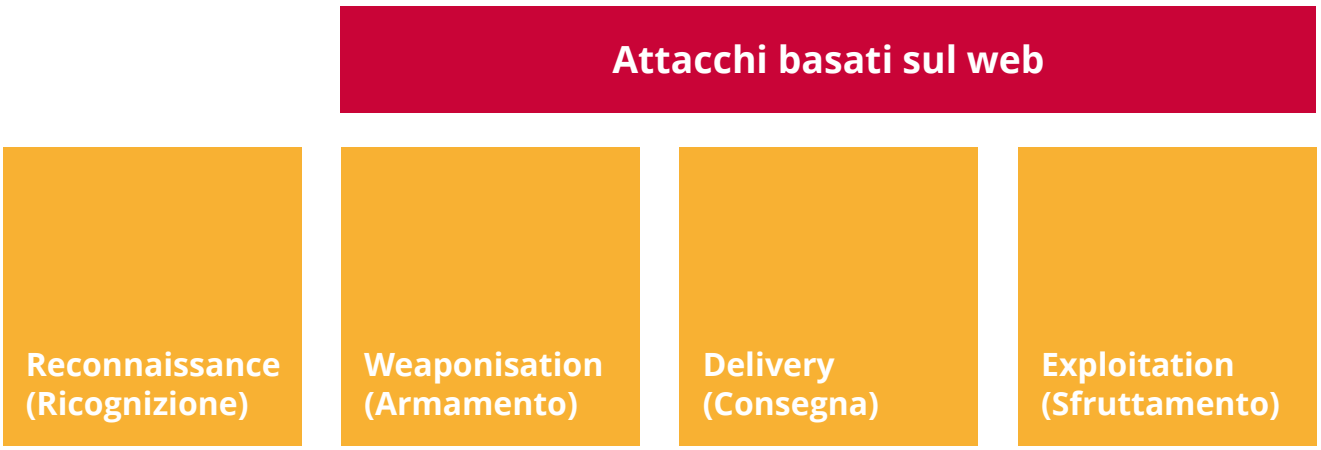
Gli attacchi di forza bruta, ad esempio, mirano a colpire un sistema operativo sovraccaricando un'applicazione web mediante tentativi di accesso con nome utente e password. Gli attacchi basati sul web possono influenzare la disponibilità di siti web, applicazioni e interfacce di programmazione delle applicazioni (API), violando la riservatezza e l'integrità dei dati.



«L’aumento della complessità delle applicazioni web e dei loro servizi diffusi pone delle sfide in termini di protezione da minacce che hanno motivazioni eterogenee, che vanno dal danno economico o reputazionale al furto di informazioni critiche o personali».

in ETL 2020

Kill chain



Fase del flusso di lavoro dell'attacco

Ampiezza dello scopo

Installazione

Command & Control (Comando e controllo)

Actions on Objectives (Azioni sugli obiettivi)

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

_A livello generale

- **IL MALWARE FORMJACKING PER IL FURTO DEI DATI DEGLI UTENTI**. L'iniezione di codice malevolo in siti web è una tecnica notoriamente utilizzata dai criminali informatici. Il formjacking è stato segnalato in passato per lo più in attività di mining di criptovalute. Tuttavia, secondo un ricercatore della sicurezza[4], si osserva uno spostamento dell'uso di questa tecnica da parte di attori malintenzionati verso i dati degli utenti e i dettagli bancari. I siti web colpiti sono rimasti infetti in media per 45 giorni. Nel maggio 2019 questo ricercatore ha segnalato il blocco di quasi 63 milioni di richieste web malevole correlate al formjacking.
- **«MAGECART» VA OLTRE E PRENDE DI MIRA LA CATENA DI FORNITURA**. Secondo un ricercatore nel campo della sicurezza, una società francese di media digitali è stata bersaglio di Group12, un attore malintenzionato che ha infettato l'inventario pubblicitario del sito, veicolando codice di skimming e colpendo migliaia di siti web che ospitavano la pubblicità.[5] Si è osservato che l'operazione di questo gruppo è stata resa più efficace grazie alla creazione dell'infrastruttura di skimming solo pochi mesi prima dell'inizio della campagna. In tal modo, l'utente finale poteva essere infettato solo visitando un sito web che ospitava questa pubblicità.[6]
- **PIATTAFORME DI COLLABORAZIONE E MESSAGGISTICA BASATE SUL WEB**. Queste piattaforme stanno diventando il ponte tra attori malintenzionati e vittime di quella che viene chiamata la backdoor SLUB. Nel marzo del 2019 un ricercatore della sicurezza si è imbattuto in una campagna che si serviva di attacchi «watering hole» per infettare le vittime, sfruttando la vulnerabilità CVE-2018-81747. L'attacco prevedeva schemi di infezione in più fasi. Un esempio del funzionamento di questi schemi è il download di un file DLL, l'uso di PowerShell per eseguirlo, il download del malware e l'esecuzione della backdoor principale. È interessante notare che il malware si collegava a un servizio di messaggistica dell'area di lavoro di Slack per inviare i risultati dei comandi, che venivano consegnati attraverso uno snippet «gist» di GitHub in cui l'aggressore aggiungeva potenzialmente comandi.[7,8]

- **ESTENSIONE DEL BROWSER, FRODE E MALVERTISING**. Un ricercatore della sicurezza ha scoperto una diffusa campagna di malvertising che si serviva delle estensioni di Google Chrome e che ha interessato circa 1,7 milioni di utenti. Queste estensioni di Chrome offuscavano la funzionalità pubblicitaria sottostante per gli utenti finali, allo scopo di mantenere il browser infetto connesso all'infrastruttura di C2. Secondo le conclusioni del ricercatore, la campagna ha intensificato l'attività tra i mesi di marzo e giugno 2019, sebbene si sospetti che fosse attiva già da molto prima.[9] Un altro ricercatore nel campo della sicurezza ha osservato un aumento dell'attività dell'adware NewTab, che utilizza le estensioni del browser, alla fine del 2019.[11]
- **GOOGLE SITES UTILIZZATO PER L'HOSTING DI PAYLOAD DRIVE-BY**. Il malware noto come «LoadPCBanker» (Win32.LoadPCBanker.Gen) è stato rilevato nel modello Schedario di Google Sites (Classic Google Sites). Secondo un ricercatore della sicurezza, l'attore ha dapprima utilizzato i Classic Google Sites per creare una pagina web e successivamente si è avvalso del modello Schedario per ospitare i payload. Ha poi utilizzato il servizio SQL come canale di esfiltrazione per l'invio e la memorizzazione dei dati delle vittime.[12,13]
- **RANSOMWARE UTILIZZA IL CONVERTITORE VIDEO ONLINE COME MECCANISMO DI DRIVE-BY DOWNLOAD**. Secondo un ricercatore della sicurezza, ShadowGate o campagna WordJS è attivo dal 2015 e prende di mira software e siti web pubblicitari. Nel corso del 2016 è stato sviluppato l'exploit kit Greenflash Sundown per potenziare l'attività della campagna, mediante iniezione del kit in servizi pubblicitari compromessi e diffusione del ransomware. Durante il 2018 ShadowGate è stato rilevato come veicolo di cryptominer verso server dell'Asia orientale per un breve periodo di tempo. La distribuzione di ShadowGate per paese è illustrata nella figura 1 della presente relazione. Anche un altro ricercatore ha segnalato l'attività, che è stata ricondotta a onlinevideoconverter[.com] come uno dei principali siti web drive-by per veicolare l'exploit kit.[14,15,16,17,18]

Tendenze

A livello generale

- **I SISTEMI DI GESTIONE DEI CONTENUTI SONO ANCORA UN BERSAGLIO IDEALE**. Considerata la loro popolarità tra gli utenti di Internet, i sistemi di gestione dei contenuti (Content Management Systems, CMS) rappresentano un bersaglio allettante per gli attori malintenzionati. Un ricercatore della sicurezza ha riscontrato un aumento dello sfruttamento di una vulnerabilità individuata nel corso del 2018 (Drupalgeddon2), che ha preso di mira la piattaforma Drupal. Analogamente, un altro ricercatore ha osservato una tendenza a sfruttare WordPress, prendendo di mira vulnerabilità e plugin di terzi obsoleti.[19,20]

- **EXPLOIT DEL BROWSER INTERNET UTILIZZATI NEGLI ATTACCHI WATERING HOLE**. È stato osservato un attore delle minacce che stava attuando un attacco watering hole mediante un portale di notizie in lingua coreana. In questo attacco, uno script malevolo (JavaScript) è stato iniettato nella home page di un sito web automaticamente (attraverso un secondo script), controllando il browser della vittima e successivamente sfruttando una vulnerabilità di Google Chrome CVE-2019-13720. Inoltre, nel luglio del 2019 è stato scoperto che una nuova versione del malware backdoor SLUB infettava il browser della vittima (vulnerabilità di Internet Explorer CVE-2019-0752) utilizzando un sito web di watering hole specifico. In una diversa indagine, il team di sicurezza dello sviluppatore del software ha individuato una serie di siti web compromessi che venivano utilizzati in attacchi watering hole che sfruttavano le vulnerabilità dell'iPhone.[21,22]

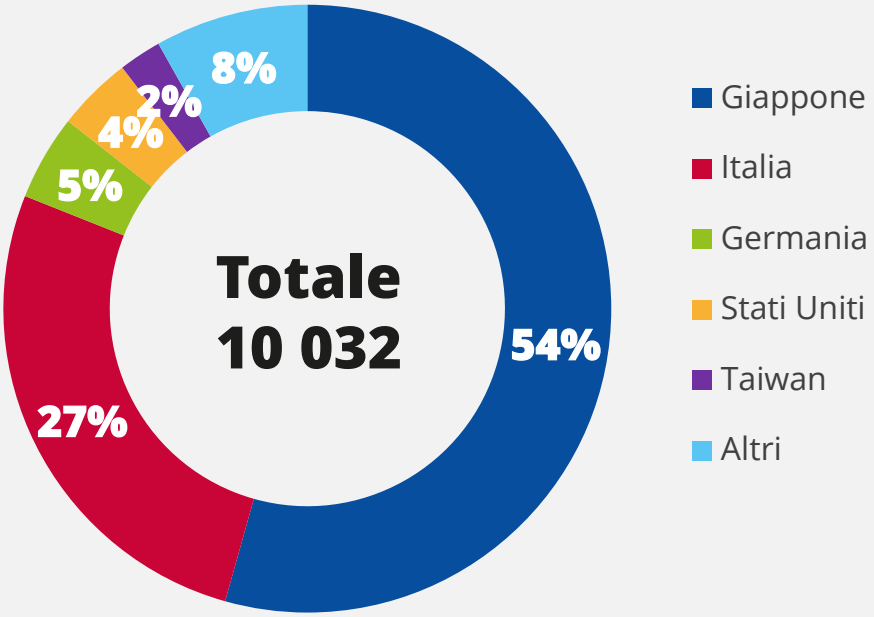


Figura 1. Distribuzione percentuale di ShadowGate per paese

Vettori di attacco

Come

- **DRIVE-BY DOWNLOAD**. Questo vettore di attacco scarica contenuti malevoli sul dispositivo della vittima. In questo tipo di attacco, è necessario che l'utente finale visiti il sito web legittimo che è stato compromesso. Perché ciò avvenga, è possibile utilizzare script malevoli iniettati nel sito web legittimo, eseguire exploit basati su browser o reindirizzare l'utente verso un sito web compromesso dietro le quinte.[25,26]
- **ATTACCHI WATERING HOLE**. Questa tecnica è impiegata per attacchi mirati mediante exploit kit con caratteristiche di tipo «stealth». In altre parole, si tratta del tipo di attacco utilizzato quando un attore malintenzionato è interessato a compromettere uno specifico gruppo di utenti, servendosi di exploit o altri contenuti malevoli (come script o pubblicità) iniettati nel sito web.[27]
- **FORMJACKING**. In questa tecnica gli attori malintenzionati iniettano codice malevolo nei moduli di pagamento di un sito web legittimo. Questo attacco cattura per lo più informazioni bancarie e altre informazioni sull'identità. In tale scenario l'utente inserisce i propri dati bancari o della carta di credito nel portale di pagamento e-commerce. Una volta raccolte e inviate le informazioni, lo script malevolo inoltra i dati contemporaneamente al portale e all'attore malintenzionato. Le informazioni vengono poi utilizzate per varie finalità criminali: guadagno economico, estorsione e vendita sui criptomercati.[3,4]
- **URL MALEVOLO**. È definito come un link creato con l'intenzione di distribuire malware o di contribuire a una truffa. Il processo prevede l'accesso con tecniche di ingegneria sociale alle informazioni della vittima, per convincerla a fare clic sull'URL malevolo, che veicola il malware o il contenuto malevolo e compromette la macchina della vittima.[28]

Operazione WizardOpium

Una vulnerabilità zero day di Google Chrome è stata riscontrata in circolazione in attacchi basati sul web mirati. La falla, registrata come CVE-2019-13720, interessa versioni precedenti a 78.0.3904.87 su sistemi Microsoft Windows, Mac e Linux. Il difetto risiede nella componente audio del browser web e, se sfruttato, può portare a un'esecuzione arbitraria di codice.

La vulnerabilità zero-day, scoperta da un ricercatore della sicurezza e registrata come CVE-2019-13720, non è stata attribuita ad alcun attore specifico, ma ricondotta a una campagna tracciata come Operation WizardOpium. Nel frattempo Google ha rilasciato un aggiornamento per la versione 78.0.3904.87 di Chrome. Secondo il ricercatore, l'attacco sfrutta un'iniezione in stile watering hole su un portale di notizie in lingua coreana. Un codice JavaScript malevolo inserito nella landing page permette di caricare lo script di profilazione da un sito remoto.[23,24]

Gli exploit del browser sono una forma di attacco che utilizza codice malevolo che sfrutta i punti deboli e le vulnerabilità del software (sistema operativo e browser) o i relativi plugin, con l'obiettivo ultimo di accedere al dispositivo della vittima.

Mitigazione

Azioni proposte

- Seguire un buon processo di gestione delle patch e pianificare;
- aggiornare il browser Internet e i relativi plugin per mantenerli aggiornati e con le patch installate contro le vulnerabilità note;
- assicurare l'installazione delle patch nelle pagine basate su sistemi di gestione dei contenuti (CMS) e nel portale, per evitare plugin e addon non verificati;
- assicurarsi che gli endpoint e il software installato siano aggiornati, dotati di patch e protetti.
- Isolare le applicazioni (whitelisting delle applicazioni) e creare una sandbox per ridurre il rischio di attacchi drive-by-compromise. Ad esempio, la tecnica di isolamento del browser può proteggere gli endpoint dallo sfruttamento del browser e dagli attacchi drive-by-compromise.[29,30,31]
- Per i proprietari di siti web, l'hardening di server e servizi è un approccio proattivo per mitigare gli attacchi basati sul web. Ciò comprende il controllo della versione degli script di contenuto, nonché la scansione dei file e degli script ospitati localmente per il server o il servizio web.[32]
- La limitazione dei contenuti basati sul web è un'altra tecnica di protezione dagli attacchi basati sul web. L'uso di strumenti come blocchi delle pubblicità o di JavaScript limiterà anche la possibilità di eseguire codici malevoli durante la visita di specifici siti web.[29,30]
- Monitorare la webmail e filtrare i contenuti per rilevare e prevenire la consegna di URL e file/payload malevoli.

«Gli attacchi basati sul web comprendono in genere tecniche quali SQL Injection, manomissione dei parametri, cross-site scripting, path traversal e forza bruta per compromettere un sistema o un'applicazione».

in ETL2020

Riferimenti bibliografici

1. «Watering Hole» Proofpoint. https://www.proofpoint.com/uk/threat-reference/watering-hole

2. «What Is a Drive-By Download?» Kaspersky. https://www.kaspersky.com/resource-center/definitions/drive-by-download

3. «Formjacking: Major Increase in Attacks on Online Retailers», Broadcom. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/formjacking-attacks-retailers

4. «What is Formjacking and How Does it Work?», Norton. https://us.norton.com/internetsecurity-emerging-threats-what-is-formjacking.html

5. «Magecart's 7 Groups: Hackers Dropping Counter-Intelligence Code in JavaScript Skimmers». 14 novembre 2018. CBR. https://www.cbronline.com/in-depth/magecart-analysis-riskiq

6. «How Magecart's Web-Based Supply Chain Attacks are Taking Over the Web». 10 marzo 2019. CBR. https://www.cbronline.com/analysis/riskiq-magecart-supply-chain-attacks

7. «CVE-2018-8174 Detail» 5 settembre 2019. NIST. https://nvd.nist.gov/vuln/detail/CVE-2018-8174

8. «Join a Slack workspace». Slack. https://slack.com/intl/en-gb/help/articles/212675257-Join-a-Slack-workspace

9. «New SLUB Backdoor Uses GitHub, Communicates via Slack» 7 marzo 2019.Trend Micros. https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/

10. «Security Researchers Partner With Chrome To Take Down Browser Extension Fraud Network Affecting Millions of Users» 13 febbraio 2020. Cisco Duo Security. https://duo.com/labs/research/crxcavator-malvertising-2020

11. «Mac threat detections on the rise in 2019» 16 dicembre 2019. Malware Bytes. https://blog.malwarebytes.com/mac/2019/12/mac-threat-detections-on-the-rise-in-2019/

12. «File Cabinet», Google. https://sites.google.com/site/tiesitestutorial/create-a-page/file-cabinet

13. Google Sites. https://sites.google.com/site/

14. «Talos ShadowGate Take Down: Global Malvertising Campaign Thwarted» 1º settembre 2016. https://blog.talosintelligence.com/2016/09/shadowgate-takedown.html

15. «New Bizarro Sundown Exploit Kit Spreads Locky» Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/

16. «Incoming! Multiple Popular Websites Attacked for Cryptocurrency Mining via GreenFlash Sundown Exploit Kit» 360 Blog. https://blog.360totalsecurity.com/en/incoming-multiple-popular-websites-attacked-cryptocurrency-mining-via-greenflash-sundown-exploit-kit/

17. «ShadowGate Returns to Worldwide Operations With Evolved Greenflash Sundown Exploit Kit» 27 giugno 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/shadowgate-returns-to-worldwide-operations-with-evolved-greenflash-sundown-exploit-kit/

18. «GreenFlash Sundown exploit kit expands via large malvertising campaign» 26 giugno 2019. Malware Bytes. https://blog.malwarebytes.com/threat-analysis/2019/06/greenflash-sundown-exploit-kit-expands-via-large-malvertising-campaign/

19. «FAQ about SA-CORE-2018-002» 28 marzo 2018. Drupal. https://groups.drupal.org/security/faq-2018-002

20. «Drupalgeddon2 still used in attack campaigns» 7 ottobre 2019. Akamai. https://blogs.akamai.com/sitr/2019/10/drupalgeddon2-still-used-in-attack-campaigns.html

21. «Trustwave Global Security Report 2019», 2019. Trustwave.

22. «Stable Channel Update for Desktop» 31 ottobre 2019. https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html

23. «Chrome 0-day exploit CVE-2019-13720 used in Operation WizardOpium». 1° novembre 2019. Kaspersky. https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/

24. «CVE-2019-13720 flaw in Chrome exploited in Operation WizardOpium attacks» 1° novembre 2019. Security Affairs. https://securityaffairs.co/wordpress/93278/hacking/cve-2019-13720-lazarus-attacks.html

25. «Web Browser-Based Attacks». Morphisec. https://www.morphisec.com/hubfs/1111/briefs/BrowserAttacksBrief-190327.pdf

26. «The 5 most common cyber attacks in 2019». 9 maggio 2019. IT Governance. https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks

27. «Exploit Kits: Their Evolution, Trends and Impact». 7 novembre 2019. Cynet. https://www.cynet.com/blog/exploit-kits-their-evolution-trends-and-impact/

28. «Web-Based Threats: First Half 2019». 1° novembre 2019. Palo Alto. https://unit42.paloaltonetworks.com/web-based-threats-first-half-2019/

29. «Mitigating Drive-by Downloads» aprile 2020. ACSC. https://www.cyber.gov.au/publications/mitigating-drive-by-downloads

30. «MITRE ATT&CK: Drive-by compromise» 5 dicembre 2019. MITRE.

https://resources.infosecinstitute.com/mitre-attck-drive-by-compromise/#gref

31. «Protecting users from web-based attacks with browser isolation» 26 settembre 2019. Shi Blog – Security Solutions. https://blog.shi.com/solutions/protecting-users-from-web-based-attacks-with-browser-isolation/

32. «https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257». 11 aprile 2019. Broadcom. https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257

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

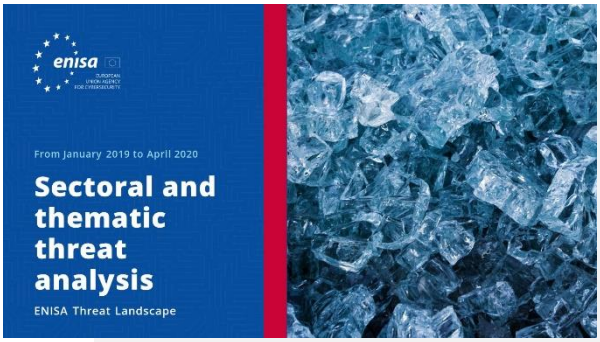
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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



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.

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