enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Webbasierte Angriffe

ENISA Threat Landscape

Überblick

Webbasierte Angriffe sind eine attraktive Methode, mit der Bedrohungsakteure Opfer täuschen können, indem sie Web-Systeme und -Dienste als Bedrohungsvektor verwenden. Dies umfasst eine große Angriffsfläche, die beispielsweise das Ermöglichen böswilliger URLs oder bösartiger Skripte ermöglicht, um den Benutzer oder das Opfer auf die gewünschte Website zu leiten, oder um schädliche Inhalte (Wasserlochangriffe[1], Drive-by-Angriffe[2]) herunterzuladen oder bösartiger Codes in eine legitime aber kompromittierte Website einzuschleusen, um Informationen zu stehlen (Formjacking[3]), einen finanziellen Vorteil zu erhalten oder sogar über Ransomware zu erpressen.[4] Zusätzlich zu diesen Beispielen sind Exploits von Internetbrowsern und Kompromisse beim Content Management System (CSM) wichtige, von verschiedenen Forschungsteams beobachtete Vektoren, die von böswilligen Akteuren verwendet werden.

Brute-Force-Angriffe zielen beispielsweise auf ein Betriebssystem ab, indem eine Webanwendung durch Anmeldeversuche mit Benutzernamen und Kennwort überwältigt wird. Webbasierte Angriffe können die Verfügbarkeit von Websites, Anwendungen und APIs (Application Programming Interfaces) beeinträchtigen und die Vertraulichkeit und Integrität von Daten verletzen.

Die zunehmende Komplexität von Webanwendungen und ihren weit verbreiteten Diensten schafft Herausforderungen bei der Sicherung derselben gegen Bedrohungen mit unterschiedlichen Motiven, von finanziellen oder Reputationsschäden bis hin zum Diebstahl kritischer oder personenbezogener Daten. “

In ETL 2020

Kill chain

Schritt des Angriffs-Workflows

Umfang des Zwecks

Installation

Command & Control

Zielführende Maßnahmen

Das Cyber Kill Chain® Framework wurde von Lockheed Martin entwickelt und basiert auf einem militärischen Konzept, das mit der Struktur eines Angriffs zusammenhängt. Um einen bestimmten Angriffsvektor zu untersuchen, verwenden Sie dieses Kill-Chain-Diagramm, um jeden Schritt des Prozesses sowie die vom Angreifer verwendeten Hilfsmittel, Techniken und Verfahren festzuhalten.

WEITERE INFORMATIONEN

Entwicklungen

_Über die Grenze

- **FORMJACKING MALWARE STIEHLT BENUTZERDATEN**. Das Einschleusen von Schadcodes in Websites ist eine bekannte Technik, die von Cyberkriminellen angewendet wird. Formjacking wurde zuvor hauptsächlich bei Cryptocurrency-Mining-Aktivitäten gemeldet. Laut einem Sicherheitsforscher[4], wechseln böswillige Akteure mit dieser Technik jedoch zu Benutzerdaten und Bankdaten. Die Zielwebsites blieben durchschnittlich 45 Tage lang infiziert. Im Mai 2019 meldete dieser Sicherheitsforscher die Blockierung von fast 63 Millionen böswilligen Webanfragen im Zusammenhang mit Formjacking.
- **„MAGECART" GEHT ÜBER DIE ZIELVERSORGUNGSKETTE HINAUS.** Laut einem Sicherheitsforscher wurde eines der französischen Unternehmen für digitale Medien von dem böswilligen Akteur „Group12" angegriffen, der das Werbeinventar der Website infizierte, Skimmer-Code lieferte und Tausende von Websites infizierte, auf denen die Werbung gehostet wurde.[5] Es wurde festgestellt, dass der Betrieb dieser Gruppe verstärkt wurde, indem die Skimming-Infrastruktur nur wenige Monate vor Beginn der Kampagne eingerichtet wurde. Dadurch konnte ein Endbenutzer nur durch den Besuch einer Website, auf der diese Werbung gehostet wird, infiziert werden.[6]
- **WEB-BASIERTE ZUSAMMENARBEITS- UND NACHRICHTENPLATTFORMEN.** Diese werden zur Brücke zwischen böswilligen Akteuren und Opfern auf der sogenannten SLUB-Hintertür. Im März 2019 stieß ein Sicherheitsforscher auf eine Kampagne, bei der Wasserlochangriffe eingesetzt wurden, um Opfer zu infizieren, indem die Sicherheitsanfälligkeit CVE-2018-81747 ausgenutzt wurde. Der Angriff umfasste einen mehrstufigen Infektionsplan. Ein Beispiel für die Funktionsweise dieses Plans ist das Herunterladen einer DLL-Datei, das Ausführen mithilfe einer PowerShell, das Herunterladen der Malware und das Ausführen der Haupt-Backdoor. Interessanterweise stellte die Malware eine Verbindung zu einem Slack Workspace-Messaging-Dienst her, um die Befehlsergebnisse zu senden, die über ein GitHub Gist-Snippet übermittelt wurden, in dem möglicherweise der Angreifer Befehle hinzufügte.[7,8]

- **BROWSER-ERWEITERUNG, BETRUG UND MALVERTISING.** Ein Sicherheitsforscher deckte eine weit verbreitete Werbekampagne mit Google Chrome-Erweiterungen auf, von der etwa 1,7 Millionen Nutzer betroffen waren. Diese Chrome-Erweiterungen verschleierten die zugrunde liegende Werbefunktion der Endbenutzer, um den infizierten Browser letztendlich mit der C2-Infrastruktur verbunden zu halten. Der Sicherheitsforscher kam zu dem Schluss, dass die Kampagne die Aktivität zwischen März und Juni 2019 erhöhte, obwohl der Verdacht bestand, dass sie lange zuvor aktiv war.[9] Ein anderer Sicherheitsforscher stellte fest, dass die NewTab-Adware-Aktivität, die Browsererweiterungen erleichtert, Ende 2019 zugenommen hat.[11]
- **GOOGLE-SEITEN FÜR DAS HOSTEN VON DRIVE-BY-PAYLOAD.** Die als „LoadPCBanker" (Win32.LoadPCBanker.Gen) bekannte Malware wurde in der Vorlage für Google Sites-Archive (Classic Google Sites) gefunden. Laut einem Sicherheitsforscher hat der Akteur zunächst die klassischen Google Sites verwendet, um eine Webseite zu erstellen, und anschließend die Vorlage für Archive zum Hosten der Nutzdaten vereinfacht. Anschließend wurde der SQL-Dienst als Exfiltrationskanal zum Senden und Speichern von Opferdaten verwendet.[12,13]
- **RANSOMWARE MIT ONLINE-VIDEOKONVERTER ALS DRIVE-BY-DOWNLOAD-MECHANISMUS.** Laut einem Sicherheitsforscher ist ShadowGate oder die WordJScampaign seit 2015 aktiv und zielt auf Werbesoftware und Websites ab. Im Laufe des Jahres 2016 wurde das Greenflash Sundown-Exploit-Kit entwickelt, um die Aktivität der Kampagne zu verbessern, indem das Kit in kompromittierte Werbedienste integriert und Ransomware verbreitet wird. Im Jahr 2018 wurde ShadowGate entdeckt, das für kurze Zeit Crypto-Miner an Server in Ostasien lieferte. Die Verteilung von ShadowGate pro Land ist in Abbildung 1 dieses Berichts dargestellt. Ein anderer Sicherheitsforscher berichtete ebenfalls über die Aktivität, die auf onlinevideoconverter [.com] als eine der wichtigsten Drive-by-Websites für die Bereitstellung des Exploit-Kits zurückgeführt wurde.[14,15,16,17,18]

Entwicklungen

Über die Grenze

- **INHALTSMANAGEMENTSYSTEME SIND NOCH IMMER EIN IDEALES ZIEL.** Angesichts der Beliebtheit von Content Management Systemen (CMS) bei Internetnutzern sind diese Systeme ein attraktives Ziel für böswillige Akteure. Ein Sicherheitsforscher identifizierte eine Zunahme der Ausnutzung einer im Jahr 2018 festgestellten Sicherheitslücke (Drupalgeddon2), die auf die Drupal-Plattform abzielt. In ähnlicher Weise beobachtete ein anderer Sicherheitsforscher einen Trend bei WordPress-Exploits, die auf Schwachstellen und veraltete Plugins von Drittanbietern abzielen.[19,20]

- **INTERNET-BROWSER-EXPLOITS FÜR WASSERLOCH-ANGRIFFE.** Ein Bedrohungsakteur wurde beobachtet, wie er über ein Nachrichtenportal in koreanischer Sprache einen Wasserlochangriff verübte. Bei diesem Angriff wurde ein bösartiges Skript (JavaScript) automatisch in die Startseite einer Website eingefügt (mithilfe eines zweiten Skripts), indem der Browser des Opfers überprüft und anschließend eine Google Chrome-Sicherheitsanfälligkeit CVE-2019-13720 ausgenutzt wurde. Darüber hinaus wurde festgestellt, dass eine neue Version der SLUB-Backdoor-Malware den Browser des Opfers (Internet Explorer-Sicherheitsanfälligkeit CVE-2019-0752) im Juli 2019 mithilfe einer bestimmten Wasserloch-Website infiziert hat. In einer anderen Untersuchung identifizierte das Sicherheitsteam des Softwareentwicklers eine Reihe kompromittierter Websites, die bei Wasserlochangriffen unter Ausnutzung von iPhone-Schwachstellen verwendet wurden.[21,22]

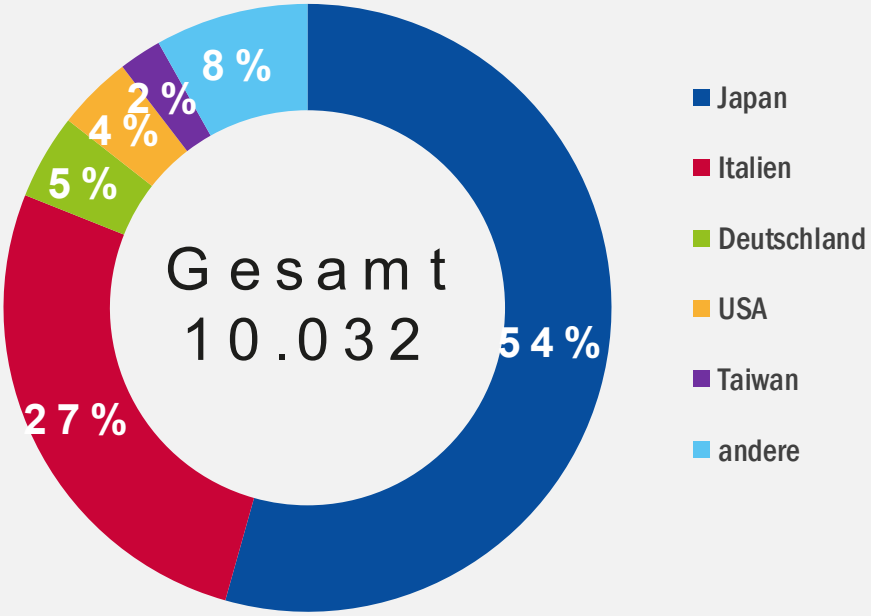


Abbildung 1: Prozentuale Verteilung von ShadowGate pro Land

Angriffsvektoren

_Wie

- **DRIVE-BY DOWNLOADS**. Dieser Angriffsvektor lädt schädliche Inhalte auf das Gerät des Opfers herunter. Bei dieser Art von Angriff muss der Endbenutzer die legitime Website besuchen, die kompromittiert wurde. Dies kann erreicht werden, indem böswillige Skripte verwendet werden, die in die legitime Website eingefügt werden, browserbasierte Exploits ausgeführt werden oder der Benutzer hinter den Kulissen auf eine gefährdete Website umgeleitet wird.[25,26]
- **WASSERLOCH-ANGRIFFE**. Diese Technik wird für gezielte Angriffe mit Exploit-Kits mit Stealth-Funktionen verwendet. Mit anderen Worten, ist es die Art von Angriff, die verwendet wird, wenn ein böswilliger Akteur daran interessiert ist, eine bestimmte Benutzergruppe mithilfe von Exploits oder anderen böswilligen Inhalten (z. B. Skripten oder Werbung), die in die Website injiziert werden, zu kompromittieren.[27]
- **FORMJACKING**. Bei dieser Technik fügen böswillige Akteure einen bösartigen Code in die Zahlungsformulare der legitimen Website ein. Dieser Angriff erfasst hauptsächlich Bank- und andere personenbezogene Daten (PII). In einem solchen Szenario gibt der Benutzer seine Bankdaten oder Kartendaten in das e-Commerce-Zahlungsportal ein. Sobald die Informationen gesammelt und übermittelt wurden, leitet das böswillige Skript die Daten gleichzeitig an das Portal und an den böswilligen Akteur weiter. Diese Informationen werden dann für verschiedene kriminelle Zwecke verwendet: Finanzielle Gewinne, Erpressung und Verkauf auf dem Dark Market.[3,4]
- **BÖSARTIGE URL**. Dies ist ein Link, der mit der Absicht erstellt wurde, Malware zu verbreiten oder einen Betrug zu ermöglichen. Der Prozess beinhaltet das Manipulieren (Social Engineering) der Informationen des Opfers, um es zu überzeugen, auf die schädliche URL zu klicken, die die Malware oder den bösartigen Inhalt liefert und den Computer des Opfers kompromittiert.[28]

Operation WizardOpium

Bei gezielten webbasierten Angriffen wurde im freien Umfeld eine Zero-Day-Sicherheitsanfälligkeit in Google Chrome festgestellt. Der als CVE-2019-13720 registrierte Fehler betrifft Versionen vor 78.0.3904.87 auf Microsoft Windows-, Mac- und Linux-Systemen. Der Fehler liegt in der Audiokomponente des Webbrowsers, und seine erfolgreiche Ausnutzung kann zu einer willkürlichen Codeausführung führen.

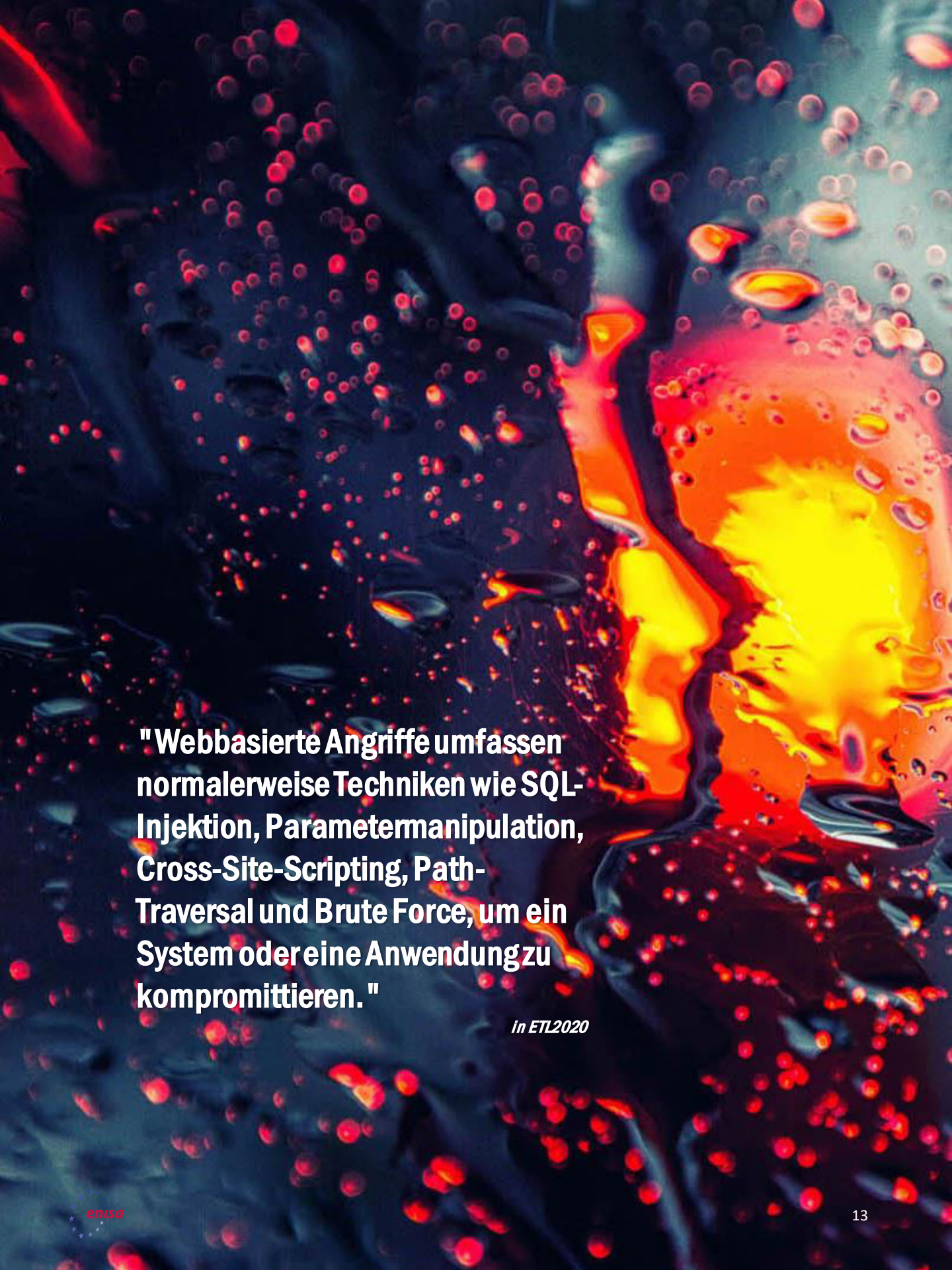
Die Zero-Day-Sicherheitsanfälligkeit, die von einem Sicherheitsforscher entdeckt und als CVE-2019-13720 registriert wurde, wurde keinem bestimmten Bedrohungsakteur zugeordnet, sondern als Teil einer Kampagne angesehen, die als Operation WizardOpium verfolgt wird. In der Zwischenzeit hat Google eine für Chrome aktualisierte Version 78.0.3904.87 veröffentlicht. Laut dem Forscher nutzt der Angriff eine Wasserlochinjektion in einem koreanischsprachigen Nachrichtenportal. Ein in die Zielseite eingefügter schädlicher JavaScript-Code ermöglicht das Laden des Profiling-Skripts von einem anderen Standort aus.[23,24]

Browser-Exploits sind eine Form der Betreibung mit bösartigem Code, bei dem Schwächen und Schwachstellen in der Software (Betriebssystem und Browser) oder verwandten Plugins verwendet werden, um letztendlich Zugriff auf das Gerät des Opfers zu erhalten.

Minderung

Vorgeschlagene Maßnahmen

- Befolgen Sie einen guten Patch-Management-Prozess und -Plan;
- Aktualisieren Sie den Internetbrowser und die zugehörigen Plugins, um sie auf dem neuesten Stand zu halten und gegen bekannte Sicherheitslücken zu patchen;
- Halten Sie die CMS-basierten Seiten (Content Management System) und das Portal gepatcht, um nicht verifizierte Plugins und Addons zu vermeiden;
- Stellen Sie sicher, dass Endpunkte und installierte Software aktualisiert, gepatcht und geschützt sind.
- Isolieren Sie Anwendungen (Whitelist für Anwendungen) und erstellen Sie eine Sandbox, um das Risiko von Drive-by-Compromise-Angriffen zu verringern. Beispielsweise kann die Browser-Isolationstechnik die Endpunkte vor Browser-Ausnutzung und Drive-by-Compromise-Angriffen schützen.[29,30,31]
- Für Websitebesitzer ist das Absichern von Servern und Diensten ein proaktiver Ansatz, um webbasierte Angriffe abzuwehren. Dies umfasst das Steuern der Version der Inhaltsskripte sowie das Scannen lokal gehosteter Dateien und Skripte nach dem Webserver oder Dienst.[32]
- Das Einschränken von webbasierten Inhalten ist eine weitere Technik zum Schutz vor webbasierten Angriffen. Durch die Erleichterung von Tools wie Adblockern oder JavaScript-Blockern wird auch die Möglichkeit eingeschränkt, beim Besuch bestimmter Websites schädliche Codes auszuführen.[29,30]
- Überwachen Sie Web-E-Mails und filtern Sie Inhalte, um die Zustellung schädlicher URLs und Dateien/Nutzdaten zu erkennen und zu verhindern.


"Webbasierte Angriffe umfassen normalerweise Techniken wie SQL-Injektion, Parametermanipulation, Cross-Site-Scripting, Path-Traversal und Brute Force, um ein System oder eine Anwendung zu kompromittieren."
in ETL2020

Literaturangaben

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. November, 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. März, 2019. CBR. https://www.cbronline.com/analysis/riskiq-magecart-supply-chain-attacks

7. "CVE-2018-8174 Detail" 5. September, 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. März, 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. Februar, 2020. Cisco Duo Security. https://duo.com/labs/research/crxcavator-malvertising-2020

11. "Mac threat detections on the rise in 2019" 16. Dezember, 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" 1. September, 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. Juni, 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. Juni, 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. März, 2018. Drupal. https://groups.drupal.org/security/faq-2018-002

20. "Drupalgeddon2 still used in attack campaigns" 7. Oktober, 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. Oktober, 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. November, 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. November, 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. Mai, 2019. IT-Governance. https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks

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

28. "Web-Based Threats: First Half 2019". 1. November, 2019. Palo Alto. https://unit42.paloaltonetworks.com/web-based-threats-first-half-2019/

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

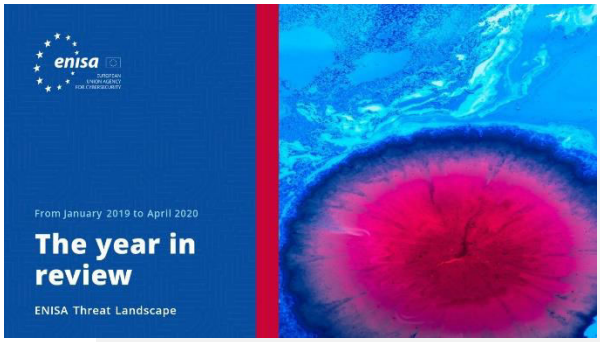
30. "MITRE ATT&CK: Drive-by compromise" 5. Dezember, 2019. MITRE.

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

31. "Protecting users from web-based attacks with browser isolation" 26. September, 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. April, 2019. Broadcom. https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257

Themenbezogen



ENISA Threat Landscape Bericht **Das Berichtsjahr**

Eine Zusammenfassung der Cybersicherheitstrends für den Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Liste der 15 größten Bedrohungen**

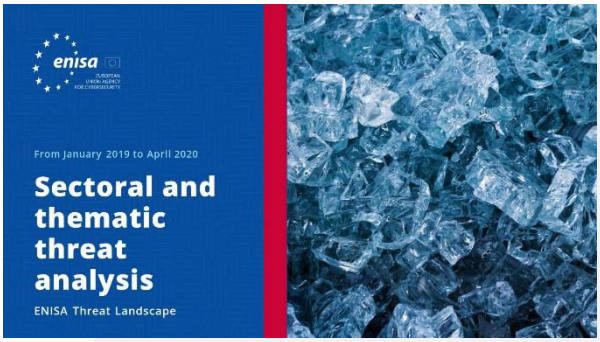
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Forschungsthemen**

Empfehlungen zu Forschungsthemen aus verschiedenen Quadranten der Cybersicherheit und Cyber Threat Intelligence.

LESEN SIE DEN BERICHT



LESEN SIE DEN BERICHT

ENISA Threat Landscape-Bericht
Sektorale und thematische Bedrohungsanalyse

Kontextualisierte Bedrohungsanalyse zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Aufkommende Trends

Die bedeutendsten Cybersicherheitstrends, die zwischen Januar 2019 und April 2020 beobachtet wurden.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Übersicht über Cyber Threat Intelligence

Der aktuelle Stand der Cyber Threat Intelligence in der EU.

Über

_ Die Agentur

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur der Europäischen Union für Cybersicherheit wurde 2004 gegründet und durch das EU-Gesetz zur Cybersicherheit gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von ICT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, sie kooperiert mit den Mitgliedstaaten und Organen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Aufbau von Fähigkeiten und Sensibilisierung in Bezug auf Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürger Europas zu gewährleisten. Weitere Information über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

Mitwirkende

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) und *alle Mitglieder der ENISA CTI Interessenvertreter:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) und Thomas Hemker.

Herausgeber

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

Kontaktangaben

Für Fragen über dieses Dokument, verwenden Sie bitte enisa.threat.information@enisa.europa.eu.
Für Medienanfragen zu dieser Stellungnahme verwenden Sie bitte die folgenden Kontaktangaben: press@enisa.europa.eu.

Wir würden gerne Ihr Feedback zu diesem Bericht erhalten!
Bitte nehmen Sie sich einen Moment Zeit, um den Fragebogen auszufüllen. Um das Formular zu öffnen, können Sie hier klicken.

Impressum/Rechtshinweise

Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung entspricht nicht unbedingt dem neuesten Stand und kann in angemessenen Abständen aktualisiert werden.

Quellen von Dritten werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung ist nur für Informationszwecke gedacht. Sie muss kostenlos zugänglich sein. Weder die ENISA noch in deren Namen oder Auftrag tätige Personen können für die Nutzung der in dieser Veröffentlichung enthaltenen Informationen haftbar gemacht werden.

Hinweis zum Copyright

© European Union Agency for Cybersecurity (ENISA), 2020 Die Vervielfältigung ist gestattet, sofern die Quelle angegeben ist.

Copyright für das Bild auf dem Cover: © Wedia. Bei Verwendung oder Wiedergabe von Fotos oder sonstigem Material, das nicht dem Urheberrecht der ENISA unterliegt, muss die Zustimmung direkt bei den Urheberrechtsinhabern eingeholt werden.

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

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

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Alle Rechte vorbehalten. Copyright ENISA 2020.

https://www.enisa.europa.eu