EN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Web-based attacks

ENISA Threat Landscape

Overview

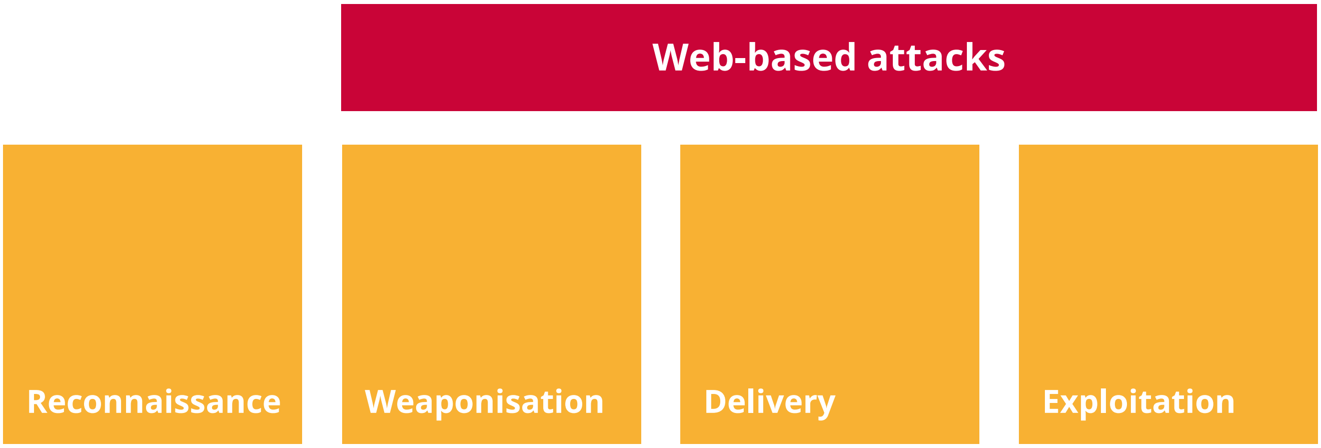
Web-based attacks are an attractive method by which threat actors can delude victims using web systems and services as the threat vector. This covers a vast attack surface, for instance facilitating malicious URLs or malicious scripts to direct the user or victim to the desired website or downloading malicious content (watering hole attacks[1], drive-by attacks[2]) and injecting malicious code into a legitimate but compromised website to steal information (i.e formjacking[3]) for financial gain, information stealing or even extortion via ransomware.[4] In addition to these examples, internet browser exploits and content management system (CSM) compromises are important vectors observed by different research teams being used by malicious actors.

Brute-force attacks, for example, target an operating by overwhelming a web application with username and password login attempts. Web-based attacks can affect the availability of web sites, applications and application programming interfaces (APIs), breaching the confidentiality and integrity of data.

“The increase in the complexity of web application and their widespread services creates challenges in securing them against threats with diverse motivations from financial or reputational damage to the theft of critical or personal information.”

in ETL 2020

Kill chain



Web-based attacks

Reconnaissance

Weaponisation

Delivery

Exploitation

🟥 *Step of Attack Workflow*

🟧 *Width of Purpose*

Installation

Command & Control

Actions on Objectives

The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.

MORE INFORMATION

Trends

_Across the board

- **FORMJACKING MALWARE STEALING USER DATA**. Injecting malicious code into websites is a well-known technique used by cybercriminals. Formjacking has been previously reported mostly in cryptocurrency mining activities. However, according to a security researcher[4], malicious actors are moving to user data and banking details using this technique. The websites targeted remained infected on average for 45 days. During May 2019, this security researcher reported the blocking of nearly 63 million malicious web requests related to formjacking.
- **'MAGECART' GOES BEYOND BY TARGETING SUPPLY CHAIN**. According to a security researcher, one of French digital media companies was targeted by the malicious actor Group12, which infected the site's advertising inventory, delivering skimmer code and infecting thousands of websites hosting the advertisement.[5] It was observed that this group's operation was made more effective by setting up their skimming infrastructure just a few months before starting the campaign. Thus, an end-user could become infected only by visiting a website hosting this advertisement.[6]
- **WEB-BASED COLLABORATION AND MESSAGING PLATFORMS**. These are becoming the bridge between malicious actors and victims on what is called the SLUB backdoor. During March 2019, a security researcher came across a campaign that was using watering hole attacks to infect victims by exploiting the vulnerability CVE-2018-81747. The attack involved multi-stage infection schemes. One example of how these schemes work is downloading a DLL file, using a PowerShell to execute it, downloading the malware and running the main backdoor. Interestingly, the malware was connecting to a Slack workspace messaging service to send the command results, which were delivered through a GitHub Gist snippet in which potentially the attacker was adding commands.[7,8]

- **BROWSER EXTENSION, FRAUD AND MALVERTISING**. A security researcher uncovered a widespread malvertising campaign using Google Chrome extensions affecting approximately 1,7 million users. These Chrome extensions were obfuscating the underlying advertising feature from the end-users to ultimately keep the infected browser connected to the C2 infrastructure. The security researcher concluded that the campaign increased activity between the months of March and June 2019, despite suspicions that it was active long before that.[9] Another security researcher observed that NewTab adware activity, which facilitates browser extensions, increased at the end of 2019.[11]
- **GOOGLE SITES USED FOR HOSTING DRIVE-BY PAYLOAD**. The malware known as 'LoadPCBanker' (Win32.LoadPCBanker.Gen) was found in Google Sites file cabinets template (Classic Google Sites). According to a security researcher, the actor first used the Classic Google Sites to create a webpage and subsequently facilitated the file cabinets template to host the payloads. Then it used the SQL service as the exfiltration channel to send and store victim data.[12,13]
- **RANSOMWARE USING ONLINE VIDEO CONVERTER AS A DRIVE-BY DOWNLOAD MECHANISM**. According to a security researcher, ShadowGate or the WordJScampaign has been active since 2015, targeting advertising software and websites. During 2016, the Greenflash Sundown exploit kit was developed to enhance the activity of the campaign by injecting the kit into compromised advertisement services and spreading ransomware. During 2018, ShadowGate was spotted delivering crypto-miners to servers in East Asia for a short time. The distribution of ShadowGate per country is presented in Figure 1 of this report. Another security researcher also reported the activity, which was tracked back to onlinevideoconverter[.com] as one of the main drive-by websites for delivering the exploit kit.[14,15,16,17,18]

Trends

_Across the board

- **CONTENT MANAGEMENT SYSTEMS ARE STILL AN IDEAL TARGET**. Considering the popularity of Content Management Systems (CMS) among internet users, these systems are an attractive target for malicious actors. A security researcher identified an increase in the exploitation of a vulnerability identified during 2018 (Drupalgeddon2) targeting the Drupal platform. Similarly, another security researcher observed an trend in WordPress exploitations targeting vulnerabilities and outdated third-party plugins.[19,20]

- **INTERNET BROWSER EXPLOITS USED IN WATERING HOLE ATTACKS**. A threat actor was seen perpetrating a watering hole attack using a Korean Language news portal. In this attack, a malicious script (JavaScript) was injected into the home page of a website automatically (leveraging a second script) by checking the victim's browser, and subsequently exploiting a Google Chrome vulnerability CVE-2019-13720. Furthermore, a new version of SLUB backdoor malware was found to be infecting the victim's browser (Internet Explorer vulnerability CVE-2019-0752) using a specific watering hole website during July 2019. In a different investigation, the security team from the software developer identified a set of compromised websites that were used in watering hole attacks exploiting iPhone vulnerabilities.[21,22]

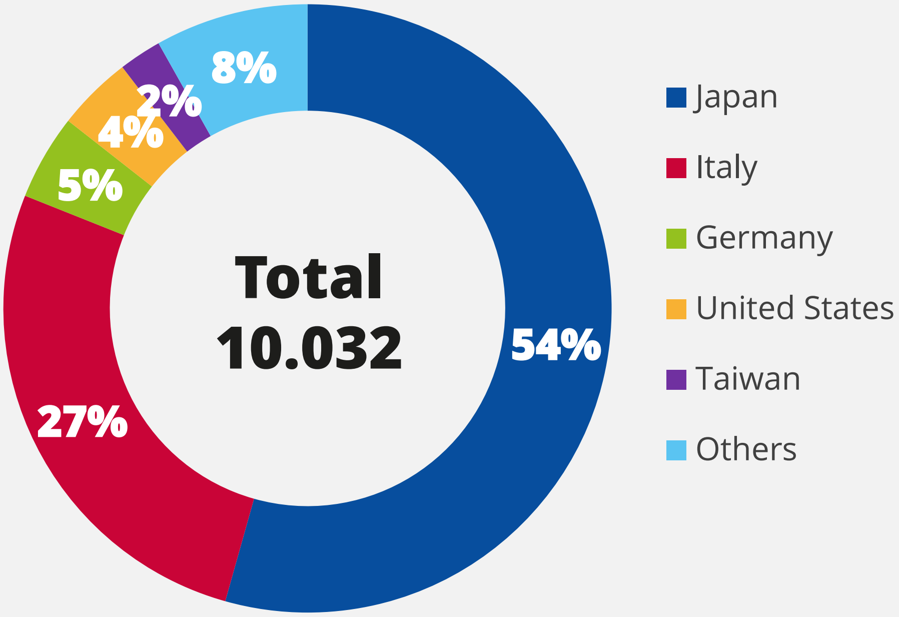


Figure 1: Percentage distribution of ShadowGate per country

Attack vectors

How

- **DRIVE-BY DOWNLOADS**. This attack vector downloads malicious contents to the victim's device. In this type of attack, the end-user needs to visit the legitimate website that has been compromised. This can be achieved by using malicious scripts injected into the legitimate website, running browser-based exploits or redirecting the user to a compromised website behind the scenes.[25,26]
- **WATERING HOLE ATTACKS**. This technique is used for targeted attacks using exploit kits with stealth features. In other words, it is the type of attack used when a malicious actor is interested in compromising a specific user group using exploits or other malicious content (i.e. scripts or advertisements) injected into the website.[27]
- **FORMJACKING**. In this technique, malicious actors inject malicious code into legitimate website's payment forms. This attack mostly captures banking and other personal identifiable information (PII). In such scenario, the user enters their banking details or card data into the ecommerce payment portal. Once the information has been collected and submitted, the malicious script will simultaneously forward the data to the portal and to the malicious actor. This information is then used for various criminal purposes: financial gain, extortion and selling it in the dark markets.[3,4]
- **MALICIOUS URL**. This is defined as a link created with the intention of distributing malware or facilitating a scam. The process involves socially engineering the victim's information to persuade them to click on the malicious URL, which delivers the malware or malicious content and compromises the victim's machine.[28]

Operation WizardOpium

A Google Chrome zero-day vulnerability was has been found in the wild in targeted web-based attacks. The flaw, registered as CVE-2019-13720, affects versions earlier than 78.0.3904.87 on Microsoft Windows, Mac and Linux systems. The defect lies in the audio component of the web browser and its successful exploitation could result in arbitrary code execution.

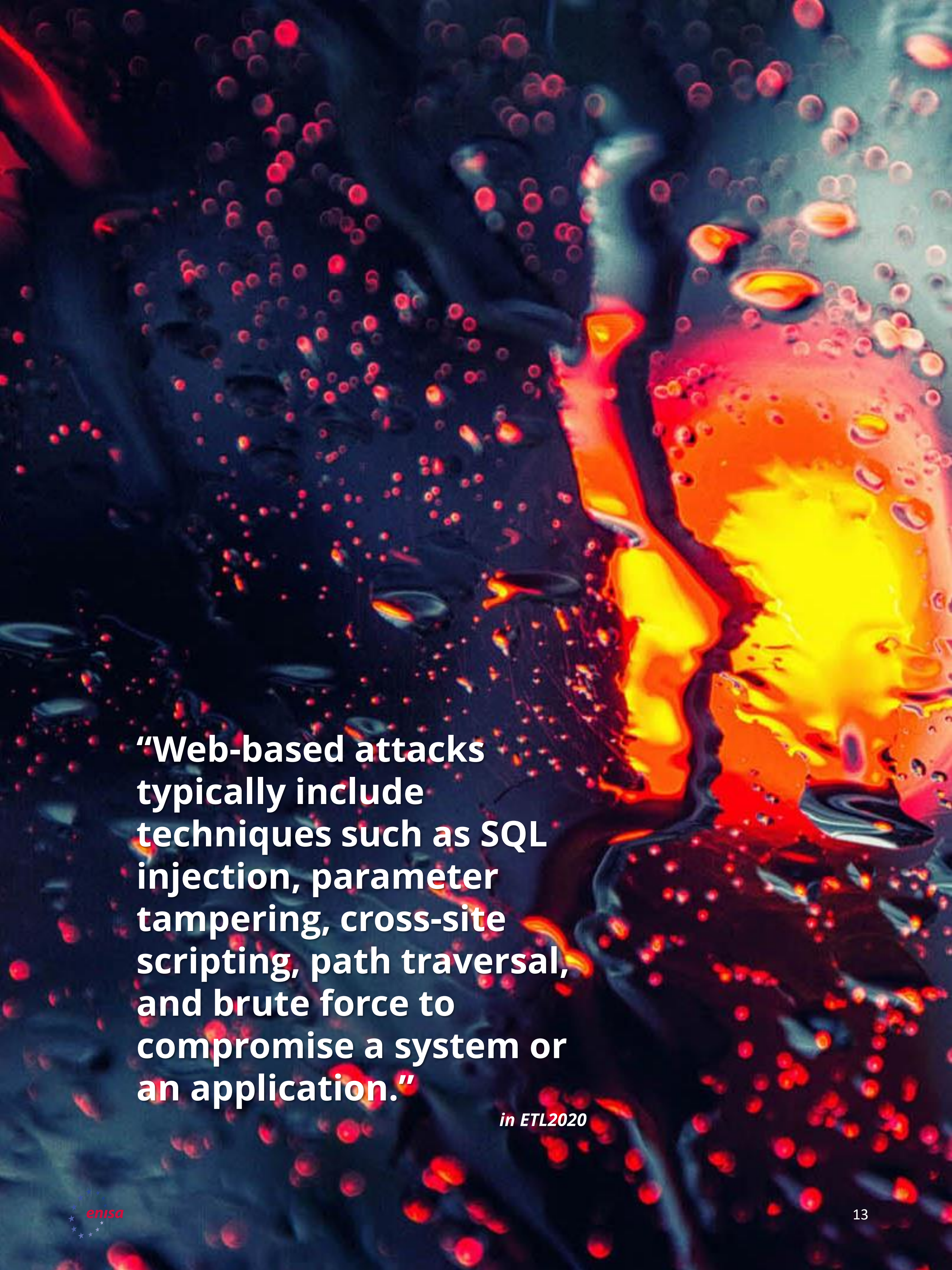
The zero-day vulnerability, discovered by a security researcher and registered as CVE-2019-13720, was not attributed to any specific threat actor but seen as part of a campaign tracked as Operation WizardOpium. In the meantime Google has released an updated for Chrome version 78.0.3904.87. According to the researcher, the attack takes advantage of a watering-hole style injection on a Korean-language news portal. A malicious JavaScript code inserted into the landing page enables the profiling script to be loaded from a remote site.[23,24]

Browser exploits are a form of exploitation using malicious code that uses weaknesses and vulnerabilities in the software (operating system and browser) or related plugins to ultimately gain access to the victim's device.

Mitigation

_Proposed actions

- Follow a good patch management process and plan;
- update the internet browser and related plugins to keep them up to date and patched against known vulnerabilities;
- keep the content management system (CMS) based pages and the portal patched to avoid unverified plugins and addon's;
- make sure that endpoints and installed software are updated, patched and protected.
- Isolate applications (application whitelisting) and create a sandbox to reduce the risk of drive-by-compromise attacks. For instance, the browser isolation technique can protect the endpoints from browser exploitation and drive-by-compromise attacks.[29,30,31]
- For website owners, hardening servers and services is a proactive approach to mitigate web-based attacks. This includes controlling the version of the content scripts as well as scanning locally hosted files and scripts for the web server or service.[32]
- Restricting web-based content is another technique for protecting against web-based attacks. Facilitating tools such as adblockers or JavaScript blockers will also limit the possibility of executing malicious codes while visiting specific websites.[29,30]
- Monitor web e-mail and filter content for detecting and preventing the delivery of malicious URLs and files/payloads.



> “Web-based attacks typically include techniques such as SQL injection, parameter tampering, cross-site scripting, path traversal, and brute force to compromise a system or an application.”

in ETL2020

References

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". November 14, 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 ". March 10, 2019. CBR. https://www.cbronline.com/analysis/riskiq-magecart-supply-chain-attacks

7. "CVE-2018-8174 Detail" September 5, 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" March 7, 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" February 13, 2020. Cisco Duo Security. https://duo.com/labs/research/crxcavator-malvertising-2020

11. "Mac threat detections on the rise in 2019" December 16, 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" September 1, 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" June 27, 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" June 26, 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" March 28, 2018. Drupal. https://groups.drupal.org/security/faq-2018-002

20. "Drupalgeddon2 still used in attack campaigns" October 7, 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" October 31, 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". November 1, 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" November 1, 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". May 9, 2019. IT Governance. https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks

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

28. "Web-Based Threats: First Half 2019". November 1, 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

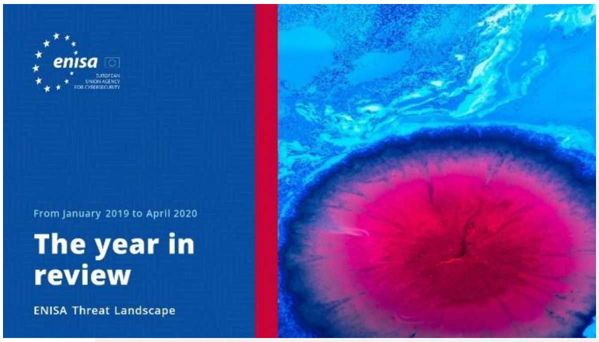
30. "MITRE ATT&CK: Drive-by compromise" December 5, 2019. MITRE.

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

31. "Protecting users from web-based attacks with browser isolation" September 26, 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". April 11, 2019. Broadcom. https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257

Related



enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

The year in review

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **The year in review**

A summary on the cybersecurity trends for the period between January 2019 and April 2020.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

ENISAs' list of top 15 threats

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **List of Top 15 Threats**

ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

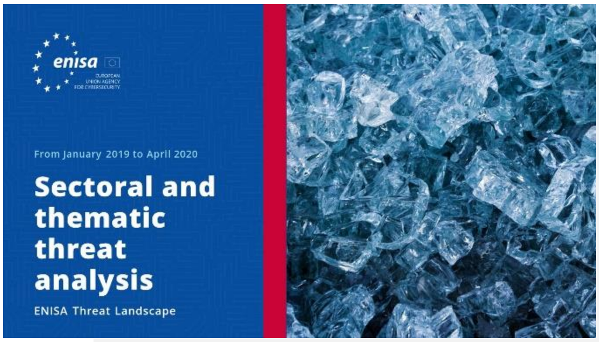
Research topics

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **Research topics**

Recommendations on research topics from various quadrants in cybersecurity and cyberthreat intelligence.



enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

Sectoral and thematic threat analysis

ENISA Threat Landscape

ENISA Threat Landscape Report **Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.

READ THE REPORT

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

Emerging trends

ENISA Threat Landscape

ENISA Threat Landscape Report **Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.

READ THE REPORT

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

Cyberthreat intelligence overview

ENISA Threat Landscape

ENISA Threat Landscape Report **Cyber Threat Intelligence overview**

The current state of play of cyberthreat intelligence in the EU.

READ THE REPORT

About

_ The agency

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contributors
Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and *all members of the ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

Editors
Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

Contact
For queries on this paper, please use enisa.threat.information@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

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

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Greece
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