enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Identitäts-diebstahl

ENISA Threat Landscape

Überblick

Identitätsdiebstahl oder Identitätsbetrug ist die illegale Verwendung der personenbezogenen Daten (PII) eines Opfers durch einen Betrüger, um sich als diese Person auszugeben und einen finanziellen und andere Vorteile zu erzielen.

Laut einem jährlichen Sicherheitsbericht wurden mindestens 900 internationale Fälle von Identitätsdiebstahl oder identitätsbezogenen Straftaten festgestellt[1]. Die wichtigsten gemeldeten Vorfälle waren:

- Die Offenlegung von fast 106 Millionen personenbezogenen Daten amerikanischer und kanadischer Bankkunden aufgrund des Vorfalls der Datenschutzverletzung von Capital One im März 2019[2];
- Die Bemächtigung von 170 Millionen Benutzernamen und Passwörtern, die der Entwickler digitaler Spiele, Zynga, im September 2019 verwendet hat;
- Der Diebstahl von 20 Millionen Konten beim britischen Audio-Streaming-Dienst Mixcloud[3];
- Die Kompromittierung personenbezogener Daten von 600.000 Fahrern und 57 Millionen Nutzern aus dem Vorfall mit Datenschutzverletzungen bei Uber im November 2019;[3]
- Der Diebstahl von 9 Millionen personenbezogenen Daten von EasyJet-Kunden, einschließlich Personalausweisen und Kreditkarten.

Der Trend des Identitätsdiebstahls spiegelt sich zu einem großen Teil in Datenschutzverletzungen wider, bei denen im Vergleich zu 2018 eine Rekordzahl von 3.800 öffentlich bekannt gegebenen Fällen, 4,1 Milliarden aufgedeckte Datensätze und ein Anstieg der Anzahl der gemeldeten Verstöße um 54 % verzeichnet wurden.[4]

Erkenntnisse

Abbildung 1: Quelle: Aus einer IBM Sicherheitsstudie - Kosten für Insider-Bedrohungen: Weltweiter Bericht[13]

Die Bedrohung durch Identitätsdiebstahl

Im Jahr 2019 wurden einige böswillige Akteure, die für größere Vorfällen aus den letzten Jahren verantwortlich waren, vor Gericht gestellt. Im Juni brachte das New Yorker Polizeipräsidium in Zusammenarbeit mit dem FBI die Mitglieder des „Fraud Ring" vor Gericht, die innerhalb und außerhalb der USA operierten und es 2012 schafften, Anmeldedaten von iPhones im Wert von 1 Million USD zu stehlen (ca. 846.000 EUR) bei einem groß angelegten Identitätsdiebstahl. Bis die Gruppe dingfest gemacht wurde, belief sich der gestohlene Gesamtbetrag auf 19 Millionen USD (ca. 16 Millionen EUR)[4]. Einen Monat später wurde die „Equifax-Einigung" öffentlich bekannt gegeben (5). Equifax musste sich bereit erklären, die US-amerikanische Federal Trade Commission, das Consumer Financial Protection Bureau, 48 Bundesstaaten, den District of Columbia und Puerto Rico für ihre Datenschutzverletzung 2017 zu entschädigen. Die Kosten beliefen sich auf mindestens 575 Millionen USD (ca. 487 Millionen EUR). Aufgrund dieser Datenschutzverletzung, die als „vollständig vermeidbar" eingestuft wurde, sickerten fast 148 Millionen amerikanische Adressen und Sozialversicherungsnummern durch. Ende des Jahres verhängte Brasilien im Namen brasilianischer Staatsbürger eine Geldstrafe in Höhe von 1,6 Millionen USD (ca. 1,35 Millionen EUR) gegen Facebook wegen des Datenlecks von Cambridge Analytica.[3]

Kill chain

Identitätsdiebstahl

Ausspähung	Wappnung	Lieferung	Betreibung

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

_Markenidentitätswechsel-Angriffe

In Übereinstimmung mit dem Trend im Jahr 2018 werden bestimmte Marken aufgrund ihres guten Rufs bei Identitätswechselangriffen bevorzugt. Obwohl diese Marken - wie Microsoft (44 %) und Amazon (17 %) - weiterhin in der Rangliste der Markenidentitätswechsel-Angriffe von 2019 führend sind, sind Neuzugänge wie der Internal Revenue Service (IRS) der Vereinigten Staaten bemerkenswert.[7] Die vertraulichen Informationen in der Lohn- und Steuererklärung (W-2) hat Betrüger schon immer angesprochen, die in diesem Berichtsjahr in 10 % der auf Identitätsbetrug basierenden E-Mails einen IRS-Identitätswechsel verwendet haben. Aus diesem Grund sind im Internet gültige W-2-Formulare und Standardformulare für die individuelle Steuererklärung (1040) zu Preisen zwischen 1 und 52 USD erhältlich.

Dieses Material ermöglicht zusammen mit den Sozialversicherungsnummern (SSN) und den Geburtsdaten, die ebenfalls verfügbar sind, jedem unerfahrenen Hacker, der bereit ist, einen Betrag von 1.000 USD (ca. 846 EUR) zu investieren, legal auf ein in den USA ansässiges Bankkonto zuzugreifen, eine falsche Steuererklärung einzureichen, eine Rückerstattung zu beantragen und eine Investition auszahlen zu lassen, die sich verdoppelt oder verdreifacht hat. Nach Angaben der IRS Criminal Investigation waren mehr als 10.000 individuelle Steuererklärungen mit Erstattungsansprüchen von mehr als 83 Millionen USD (ca. 70 Millionen EUR) potenziell betrügerisch.[9]

Der Zyklus der Schritte für den Steuerbetrug „Dirty Dozen"

Abbildung 2 - Quelle: BDO[19]

Entwicklungen

_SIM-Austausch von Identitäten

Diese Technik wird seit 2016 verwendet und richtet sich an Inhaber von Kryptowährungen. Im Jahr 2019 wurde dieselbe Technik jedoch gegen hochkarätige Personen oder Konten angewendet, um die Identität des Opfers zu stehlen. Eine Reihe von Opfern des SIM-Austauschs wurde registriert, darunter Jack Dorsey (CEO von Twitter), Jessica Alba (Schauspielerin), Shane Dawson (Schauspieler), Amanda Cerny (Schauspielerin, zweimal Opfer), Matthew Smith (Schauspieler, viermal Opfer)) und King Bach (Künstler).[10] In zwei Fällen wurde das SIM-Tauschen auch in großem Umfang eingesetzt: Bei Mosambiks größter Bank, wo bis zu 50.000 USD (ca. 42.300 EUR) von hochkarätigen Geschäftskonten gestohlen wurden, und in Brasilien, wo die Konten von 5.000 Opfern, hauptsächlich Politiker, Minister und Gouverneure, gehackt wurden.[11]

_Geschenkkarten, die als Trojaner für Business-E-Mail-Kompromittierungen (BEC) verwendet wurden

BEC-Angriffe verursachten 2019 Verluste in Milliardenhöhe. In solchen Fällen geben sich die Angreifer als vertrauenswürdige Person aus, normalerweise innerhalb des Unternehmens, und das Opfer wird dazu verleitet, eine finanzielle Transaktion durchzuführen oder vertrauliche persönliche oder geschäftliche Informationen preiszugeben. Bei mehr als der Hälfte der BEC-Angriffe wurde das Opfer zum Kauf einer Geschenkkarte verleitet. Während des Kaufvorgangs wurden vertrauliche Informationen wie Anmeldedaten des Bankkontos abgefangen. Das Opfer war auch gezwungen, die Geschenkkarte als anonyme, irreversible und direkte Auszahlungsoption an den Angreifer zu senden. Der durchschnittliche Betrag, der pro Geschenkkarte gestohlen wurde, erreichte 1.500 USD (ca. 1.269 EUR).[12]

Erkenntnisse

20 %_ von Identitätsbetrug-Angriffen verwendeten kompromittierte Konten[7]

30 %_ der Angriffe auf Konten von Führungskräften auf C-Ebene wurden durch Täuschung des Anzeigenamens kompromittiert[7]

65 %_ von BEC-Angriffen verleiteten Opfer zum Kauf von Geschenkkarten[12]

€3,32_ Millionen Kosten im Durchschnitt für eine Datenschutzverletzung

95 %_ der Befragten einer Eurobarometer-Umfrage sehen Identitätsdiebstahl als schweres Verbrechen an

Entwicklungen

Digitale Doppelgänger

Die Betrugsbekämpfungstechnik „Digitale Masken“ wurde aufgedeckt, als im April 2019 mehr als 60.000 gestohlene digitale Identitäten als Handelsprodukt auf dem Darknet-Marktplatz Genesis auftauchten. Diese Doppelgänger waren für jeweils 5 bis 200 USD erhältlich. Der Besitzer eines Doppelgängers kann einen echten Benutzer in einem Online-Shop oder Zahlungsdienst leichter nachahmen, insbesondere wenn dies mit gestohlenen Anmeldedaten und Passwörtern kombiniert wird. Neben dem Kauf digitaler Doppelgänger sind neue Instrumente zur Unterstützung des potenziellen Imitators erschienen, wie beispielsweise der Tenebris-Browser, in den ein Generator eingebettet ist, mit dem die einzigartigen Fingerabdrücke und digitalen Masken entwickelt werden können.[11]

In den letzten Jahren wurden Skimmer, Dumpster Diver, Hacker, Administratorimitatoren und Phisher als Hauptgruppen für die Angriffe auf Identitätsdiebstahl identifiziert. Diese Liste wurde 2019 um Visher und Smisher erweitert. Visher phischen über Telefonanrufe. Im Gegensatz zu Telefonimitatoren geben Visher vor, eine bekannte Organisation zu repräsentieren, und bieten an, das Opfer mit einem Service zu unterstützen, beispielsweise der Verwaltung von Computersoftware, Finanzen oder einer Steuerrückerstattung. Smisher senden falsche SMS-Nachrichten, und wenn der Empfänger antwortet, wird sein Gerät direkt gekapert oder auf eine Phishing-Website umgeleitet.

Die folgende Abbildung zeigt die häufigsten Datentypen, die 2019 verloren gegangen sind, wobei E-Mail-Daten die höchste Anzahl verlorener oder gestohlener Datensätze ausmachen. Diese Zahlen zeigen den Ernst der Lage, wenn man bedenkt, dass E-Mails persönliche, geschäftliche und behördliche sensible Informationen enthalten können.

Top-Datentypen, die im Jahr 2019 verloren gingen

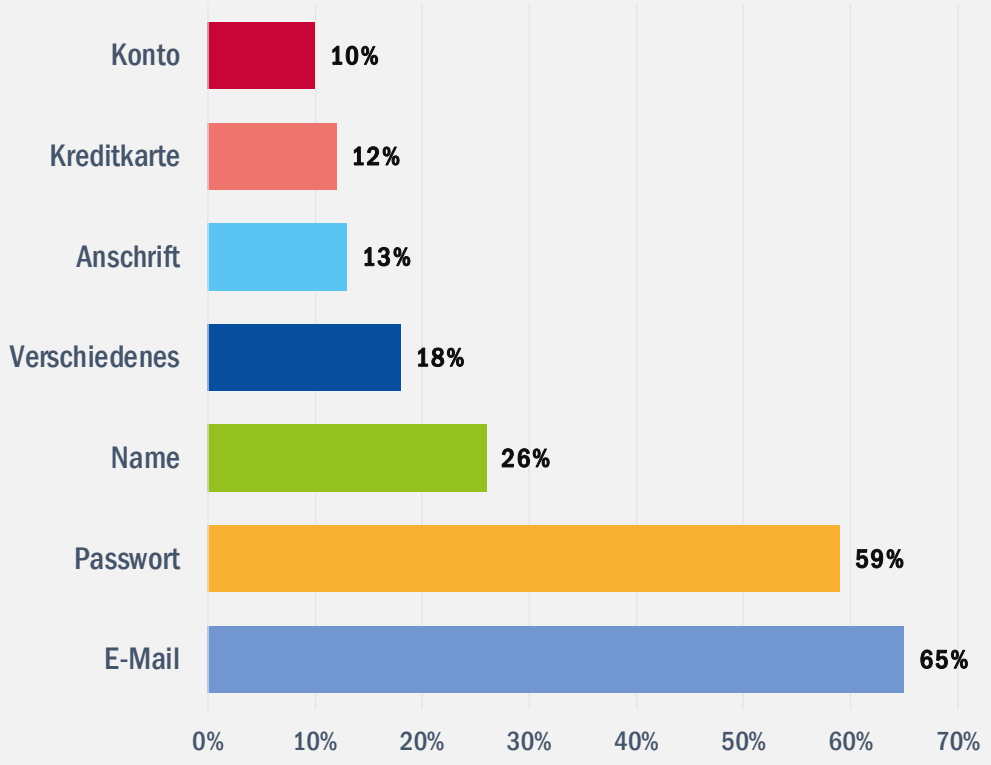


Abbildung 3 - Quelle RiskBased SECURITY[8]

Angriffsvektoren

Wie

- **DIE CLOUD ALS ANGRIFFSOBERFLÄCHE FÜR KUNDENDATEN.** Im Berichtsjahr wurde Amazon CloudFront, ein Content Delivery Network (CDN), kompromittiert.[14] Die Websites, die in der Amazon-Infrastruktur gehostet oder mit Bibliotheken verknüpft wurden, wurden freigelegt und enthüllten extern geladene Inhalte, einschließlich Kreditkartendaten.
- **PHISHING URL.** Die gängigen Malware-URL-Techniken[16] für Domain-Squatting, Domain-Shadowing und URL-Shortener wurden 2019 erneut verwendet. Im letzten Quartal 2019 wurde festgestellt, dass 26 % der böswilligen Domänen ein sicheres Zertifikat verwendeten und jedes dritte dieser Zertifikate SSL war. Dieser Trick beeinträchtigte das Urteil der Besucher, die sich aus Sicherheitsgründen auf das Vorhängeschlosssymbol in ihren Browsern verlassen hatten.[15]
- **W2 SCAM.** Ein weiterer Angriff, der auf die Aufzeichnungen von Unternehmen und Organisationen abzielt, um auf vertrauliche Informationen zuzugreifen, ist der W2-Betrug. Der Betrug beginnt damit, dass ein leitendes Mitglied der Finanz- oder Personalabteilung vorgetäuscht wird, um die Unterlagen der Mitarbeiter zu erhalten. Diese Datensätze werden dann für Identitätsdiebstahl verwendet. Der Betrug ist nach dem amerikanischen W2-Steuerformular benannt, mit dem die Löhne der Mitarbeiter gemeldet werden. Obwohl dieser Betrug im Bereich Social Engineering alt ist (erstmals 2016 von IRS gemeldet), ist sein Vorkommen in den letzten Jahren jedes Jahr um 10 % gestiegen.[9,17]
- **NIMCY.** Im Jahr 2019 wurde Nimcy, ein Spear-Phishing-Tool, von der Gruppe eingeführt, die auch für die Zebrocy-Malware-Familie verantwortlich ist. Es wurde mit der Programmiersprache Nim (ehemals Nimrod) entwickelt, die von derselben Gruppe von Hackern erstellt wurde. Dieser neue Downloader und diese neue Hintertür wurden verwendet, um Anmeldedaten, Tastenanschläge, Mitteilungen und Dateien von Diplomaten, Verteidigungsbeamten und Mitarbeitern des Ministeriums im Bereich Außenpolitik zu stehlen. Die Angreifer schienen sich auf zentralasiatische Regierungen zu konzentrieren, wobei Pakistan und Indien bevorzugt wurden.[14]

- **MOBILE BEDROHUNGEN.** Ein Anstieg bösartiger mobiler Apps wurde 2019 festgestellt und setzte sich 2020 fort. Sogar weit verbreitete und vertrauenswürdige Plattformen wie Google Play hosten Apps, die darauf abzielen, Anmeldedaten zu stehlen (z. B. Acesse SantaMobile, Modulo ID). Die Anzahl der Downloads war jedoch äußerst gering, was zeigt, dass die potenziellen Opfer nicht getäuscht wurden.[20]
- **TROJAN-BANKER.ANDROIDOS.SVPENG.AK** Der achtbeliebteste mobile Trojaner und der beliebteste mobile Banking-Trojaner, der für 1,75 % bzw. 16,85 % der eindeutigen Angriffe verantwortlich ist und hauptsächlich auf die Bankdaten der Opfer und die Zwei-Faktor-Autorisierungscodes abzielt. Die Mehrheit der Opfer dieses Trojaners befindet sich in Russland, was es zum Top-Land in Bezug auf den Anteil der Benutzer macht, die von Mobile-Banking-Trojanern angegriffen werden.[21]
- **FORMJACKING.** Formjacking war 2018 sehr verbreitet, aber die Anzahl der Angriffe schien im ersten Quartal 2019 erheblich zu sinken. Ab Mai stieg jedoch mit dem Angriff auf einen amerikanischen Gesundheitsdienstleister und dem Diebstahl von Anmeldedaten die Anzahl der Angriffe im weiteren Jahresverlauf weiter an. In diesem Monat wurde eine Allzeithochzahl von 1,1 Millionen Entdeckungen verzeichnet. Die fünf Länder mit den meisten Formjacking-Erkennungen im Jahr 2019 waren die USA (51,8 %), Australien (8,1 %), Indien (5,7 %), das Vereinigte Königreich (4,1 %) und Brasilien (3,5 %). Die Megacart-Hacker-Gruppe ist stark mit der Entwicklung von Formjacking-Tools und den Angriffen auf British Airways, Newegg, Feedify und Ticketmaster verbunden.[22]

Minderung

Vorgeschlagene Maßnahmen

- Vermeiden Sie die Verwendung des vom Browser bereitgestellten Passwort-Managers. Verwenden Sie bei Bedarf einen offline geschützten Passwortmanager.[23]
- Authentifizieren Sie jeden Absender einer Anfrage zur Überweisung von Geld per Telefon oder persönlich.[19]
- Geben Sie keine vertraulichen Informationen wie Patientenakten in handschriftlichen Notizen weiter, um deren Verlust oder Verlegung zu verhindern. Digitale Dateien eignen sich besser für Daten mit kurzer Lebensdauer und sollten dann vollständig zerstört werden.
- Verwenden Sie „Threat Hunting" in Ihrem Unternehmen, um die Sicherheitspläne zu stärken. Threat Hunting wird von erfahrenen Mitgliedern des SOC-Teams (Security Operation Center) durchgeführt, um Schwachstellen proaktiv zu identifizieren und zu verhindern, dass sie ausgenutzt werden.
- Verwenden Sie Richtlinien wie geschwindigkeitsbasierte Regeln, um Identitätsbetrug zu minimieren, insbesondere bei Kartenzahlungstransaktionen. Die Maschinendaten gültiger Transaktionen können ausreichende Informationen für eine optimale Richtliniendefinition liefern.
- Verwenden Sie, sofern verfügbar, die SSO-Authentifizierungsmethode (Single Sign-On), mit der ein Benutzer auf mehrere Anwendungen mit denselben digitalen Anmeldeinformationen zugreifen kann. Die Verwendung wird dringend empfohlen, um die Anzahl der Benutzerkonten und gespeicherten Anmeldedaten zu minimieren.
- Installieren Sie den Endpunktschutz mithilfe von Antivirenprogrammen, blockieren Sie jedoch auch die Ausführung von Dateien entsprechend (z. B. blockieren Sie die Ausführung im temporären Ordner).
- Die Multi-Faktor-Authentifizierung ist eine Sicherheitsmaßnahme, um das Hacken oder Verlieren von Passwörtern zu verhindern und den Erfolg des Authentifizierungsprozesses mit mehreren Schlüsseln sicherzustellen. Durch die Einführung der adaptiven Multi-Faktor-Authentifizierung wird der Authentifizierungsprozess basierend auf dem Verhalten des Benutzers und dem zugehörigen Kontext optimiert.

- Überprüfen Sie URLs, die per E-Mail gesendet oder zufällig besucht werden, basierend auf ihrer IP-Adresse, dem mit der IP verknüpften Lieferavis, dem Eigentümer der Domain und der Beziehung zwischen dieser Domain und anderen, bevor weitere Schritte unternommen werden.
- Unternehmen, die Cloud-Dienste nutzen, sollten über starke Cloud-Sicherheitsvorgänge verfügen und vorzugsweise gleichzeitig eine Architektur aus lokalem Speicher, privatem Cloud-Speicher und öffentlichem Cloud-Speicher verwenden, um die personenbezogenen Daten ihrer Kunden zu schützen.
- Erzwingen Sie die Verwendung starker und aktualisierter Verschlüsselungsmethoden wie TLS 1.3 (unter Verwendung kurzlebiger Schlüssel) für vertrauliche Daten, um Hacking zu verhindern.
- Schützen Sie alle Ausweisdokumente und Kopien (physisch oder digital) zureichend vor unbefugtem Zugriff.
- Geben Sie keine Identitätsinformationen an unerwünschte Empfänger weiter, und Anfragen per Telefon, E-Mail oder persönlich sollten nicht beantwortet werden.
- Erzwingen Sie die Verwendung passwortgeschützter Geräte, stellen Sie eine gute Qualität der Anmeldeinformationen und sichere Methoden für deren Speicherung sicher.
- Stellen Sie eine gute Qualität der Anmeldedaten und sichere Methoden für deren Speicherung auf allen verwendeten Medien sicher.
- Achten Sie genau darauf, wenn Sie öffentliche Wi-Fi-Netzwerke verwenden, da Betrüger sie hacken oder nachahmen. Wenn Sie ein solches verwenden, vermeiden Sie den Zugriff auf sensible Anwendungen und Daten. Verwenden Sie einen vertrauenswürdigen VPN-Dienst, um eine Verbindung zu öffentlichen Wi-Fi-Netzwerken herzustellen.
- Überprüfen Sie Transaktionen, die durch Kontoauszüge dokumentiert sind oder bei denen regelmäßig Belege anfallen, auf Unregelmäßigkeiten.
- Installieren Sie eine Inhaltsfilterung, um unerwünschte Anhänge, E-Mails mit schädlichem Inhalt, Spam und unerwünschten Netzwerkverkehr herauszufiltern.
- Erzwingen Sie die Verwendung von DLP-Lösungen (Data Loss Prevention).

Literaturangaben

1. "2019 identity theft report released" 31. Juli, 2019. ITIJ. https://www.itij.com/latest/news/2019-identity-theft-report-released

2. "Capital One data breach: What you can do now following bank hack" 12. August, 2019. C | Net. https://www.cnet.com/how-to/capital-one-data-breach-what-you-can-do-now-following-bank-hack/

3. "Cybercrime Diary, Vol. 4, No. 4: Who's Hacked? Latest Data Breaches And Cyberattacks". 8. Januar, 2020. Cyber crime Magazine. https://cybersecurityventures.com/cybercrime-diary-q1-2020-whos-hacked-latest-data-breaches-and-cyberattacks/

4. "$19 million worth of iPhones stolen in massive identity theft scam" 15. Juni, 2019. 9To5Mac. https://9to5mac.com/2019/06/05/19-million-worth-of-iphones/

5. "Equifax to pay at least $575 million as part of FTC settlement " 22. Juli, 2019. C | Net. https://www.cnet.com/news/equifax-to-pay-at-least-575m-as-part-of-ftc-settlement/

6 "2019 data breaches: 4 billion records breached so far" Norton. https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

7. "Q1 2019: Email Fraud and Identity Deception Trends" Agari. https://www.agari.com/insights/ebooks/2019-q1-report/

8. "Data Breach QuickView Report, 2019 Q3 trends." November 2019: RiskBased SECURITY. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf

9. "IRS issues 2019 annual report; highlights program areas across the agency" 6. Januar, 2020. IRS. https://www.irs.gov/newsroom/irs-issues-2019-annual-report-highlights-program-areas-across-the-agency

10. "Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too" 5. September, 2019. The New York Times. https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html

11. "IT threat evolution Q2 2019" 19. August, 2019. Kaspersky. https://securelist.com/it-threat-evolution-q2-2019/91994/

12. "Phishing Activity Trends Report" 12. September, 2019. Anti-phishing Working Group. https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf

13. "The Cost of Insider Threats" IBM. https://www.ibm.com/downloads/cas/LQZ4RONE

14. "APT trends report Q2 2019" 1. August, 2019. Kaspersky. https://securelist.com/apt-trends-report-q2-2019/91897/

15. "Proof Point Q3 2019 threat report: Emotets return, rats reign supreme and more" Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

16. ENISA Threat Landscape Report 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

17. "Q2 2019 Cryptocurrency Anti-Money Laundering Report" CipherTrace. https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/

18. "Latest Quarterly Threat Report - Q1 2019" Proof Point. https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

19. "BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare" Oktober, 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

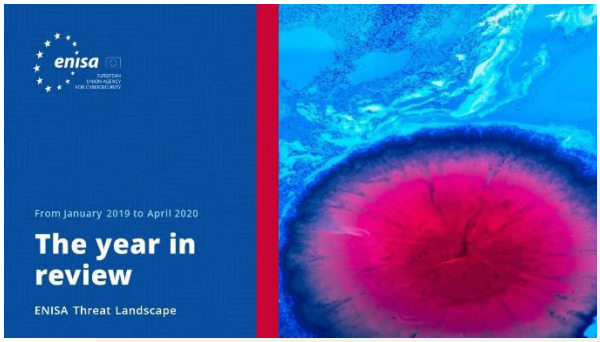
20. "IT threat evolution Q1 2019. Statistics" 23. Mai, 2019. Kaspersky. https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

21. "IT threat evolution Q3 2019. Statistics" 29. November, 2019. Kaspersky. https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

22. "FORMJACKING: How Malicious JavaScript Code is Stealing User Data from Thousands of Websites Each Month" August 2019. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-formjacking-deep-dive-en.pdf

23. "Tax Fraud & "Identity Theft On Demand" Continue to Take Shape on the Dark Web" VMWare. https://www.carbonblack.com/resources/threat-research/tax-fraud-identity-theft-dark-web/

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**

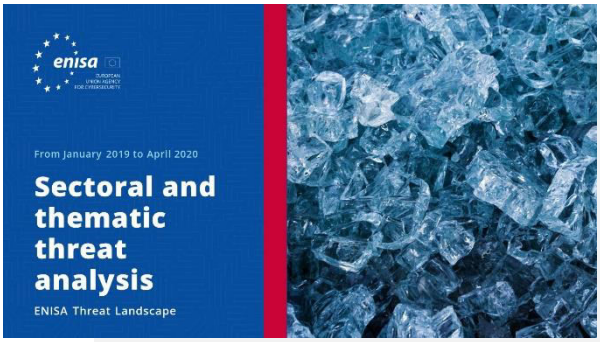
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

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.

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

https://www.enisa.europa.eu