DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Avast-Bedrohungsbericht Q3/2023

Avast-Bedrohungsbericht Q3/2023

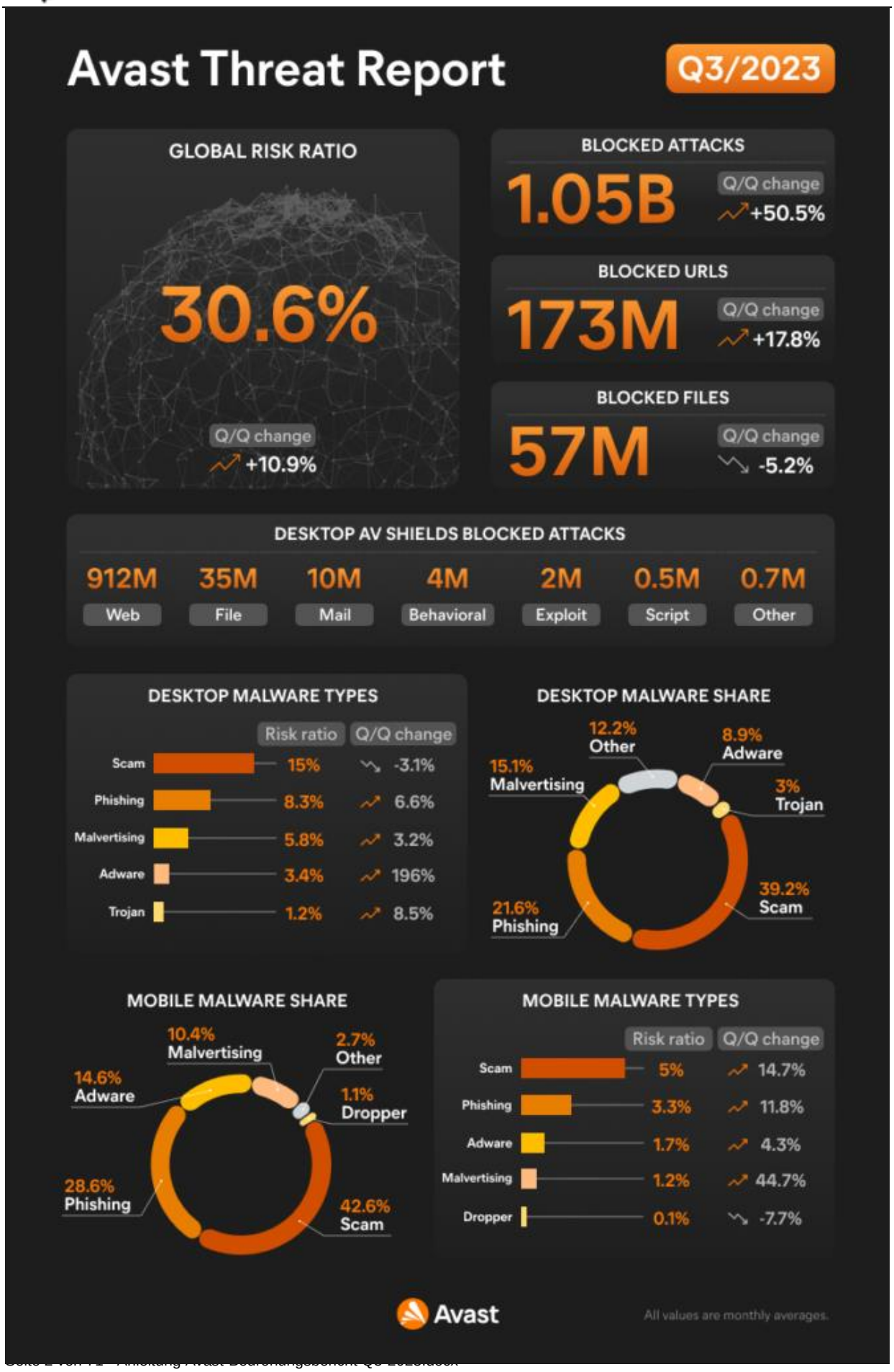
von Threat Research Team, 16. November 2023, 65 Min. Lesezeit

Atemberaubender Anstieg der geblockten Angriffe um 50 %, was zu 1 Milliarde monatlichen Blockaden führt

Vorwort

Wenn wir uns mit dem Bedrohungsbericht für das dritte Quartal 2023 befassen, wird deutlich, dass das vergangene Quartal kein gewöhnliches war. Normalerweise führt die Urlaubszeit zu einem Rückgang der Online-Aktivitäten und bietet eine kurze Pause von Cyber-Bedrohungen. In diesem Jahr nahm die digitale Landschaft jedoch eine unerwartete Wendung. Trotz der reduzierten Online-Präsenz verzeichneten unsere Erkennungssysteme einen atemberaubenden Anstieg der einzelnen blockierten Angriffe um 50 %, was zu neuen Allzeithochs führte. durchschnittlich **Im dritten Quartal 2023 haben wir** jeden Monat über eine Milliarde einzigartige Malware-Angriffe blockiert . Der Anstieg wurde durch einen erheblichen Anstieg webbasierter Bedrohungen, insbesondere Social Engineering und Malvertising, vorangetrieben. Folglich liegt die Gesamtrisikoquote, die das Risiko darstellt, von uns ins Visier genommen und geschützt zu werden, mittlerweile bei über 30 %.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55



Der Einsatz von KI durch Bedrohungsakteure, insbesondere bei Deepfake-Finanzbetrügereien, nimmt zu. Der schändliche Einsatz von Deepfakes, die auf TikTok-Benutzer abzielen und häufig Persönlichkeiten des öffentlichen Lebens wie Elon Musk darstellen, gibt zunehmend Anlass zur Sorge. Mehr dazu finden Sie in unserem Abschnitt „Empfohlene Geschichten“.

Darüber hinaus war die Bedrohungslandschaft durch eine Verdoppelung des Adware-Bedrohungsniveaus gekennzeichnet, was auf eine erhebliche Eskalation von Adware hindeutet. Südamerika, Afrika, Südosteuropa und Ostasien trugen die Hauptlast dieses Anstiegs.

Abgesehen von Adware gab es bedeutende Entwicklungen im Bereich der Botnetze. Der Versuch des FBI, das Qakbot-Botnetz zu zerschlagen, führte zu einem spürbaren Rückgang der Aktivität. Allerdings scheint die Operation noch nicht vollständig ausgelöscht zu sein, da einige damit verbundene Bedrohungsakteure bereits begonnen haben, auf alternative Formen wie DarkGate umzusteigen.

Darüber hinaus verzeichneten Informationsdiebe einen erheblichen Anstieg der Risikoquote, wobei die Ukraine (44 %), die Vereinigten Staaten (21 %) und Indien (16 %) die stärksten Anstiege verzeichneten. AgentTesla dominierte diese Landschaft, während der einst berüchtigte Raccoon Stealer an Schwung zu verlieren scheint und von der vordersten Front zurücktritt.

Auch Remote Access Trojaner (RATs) liegen weiterhin im Trend. Der Anstieg von RATS, der erstmals im zweiten Quartal 2023 beobachtet wurde, setzte sich im dritten Quartal 2023 fort, hauptsächlich angetrieben durch Remcos RAT und Warzone. Länder wie Portugal (148 % Anstieg), Polen (55 %) und die Slowakei (43 %) verzeichneten einen deutlichen Anstieg der Angriffe. Der XWorm-Stamm bleibt produktiv, veröffentlicht ständig neue Versionen und erweitert seine Reichweite.

Darüber hinaus erregte das Auftauchen einer neuen Schwachstelle, CVE-2023-38831, in der beliebten WinRAR-Software die Aufmerksamkeit von Bedrohungsakteuren, darunter APTs, RATs und Malware-Downloader. Angesichts der weiten Verbreitung der Software ist es wahrscheinlich, dass diese Exploits fortbestehen, was unterstreicht, wie wichtig es ist, die Software auf dem neuesten Stand zu halten. Weitere Informationen zu diesen Schwachstellen finden Sie in unserem Abschnitt „Exploits“.

Der Bereich der Betrügereien hat erhebliche Veränderungen erfahren, wobei Dating-Betrügereien im Vergleich zum Vorquartal einen Anstieg von 34 % verzeichneten. Belgien, Deutschland, Kanada und die Vereinigten Staaten gehören zu den Hauptzielen dieser Betrüger. Um die Herausforderung noch zu verschärfen, haben unsere Forscher eine neue Bedrohung entdeckt, die wir Love-GPT genannt haben. Dieses KI-gesteuerte Tool unterstützt Bedrohungsakteure bei der Erstellung realistischer Personas und steigert so den Erfolg ihrer betrügerischen Aktivitäten.

Phishing-Angriffe verzeichneten ebenfalls einen vierteljährlichen Anstieg von 14 %, wobei Bedrohungsakteure auf innovative Weise IPFS (InterPlanetary File System) nutzen, um herkömmliche Abwehrmechanismen zu umgehen. Insbesondere in Australien kam es zu einem erheblichen Anstieg gezielter E-Mail-Betrügereien.

Schließlich bleibt die mobile Bedrohungslandschaft dynamisch und von Spionagetaktiken geprägt. Als Reaktion auf die eskalierenden Spannungen zwischen Israel und Palästina entstand

Spyware, die eine in Israel verwendete Raketenwarnanwendung nachahmte, mit dem Ziel, Opferdaten zu stehlen. Auch die Einführung von Invisible Adware mit über zwei Millionen Downloads aus dem Google PlayStore trug zum steigenden Risiko mobiler Adware bei. Brasilien, Indien und Argentinien bleiben die am stärksten betroffenen Länder. Außerdem wird die Lücke, die durch die Abschaltung von FluBot bei Mobile-Banking-Trojanern entstanden ist, nach und nach geschlossen. In diesem Quartal wurden neue und wiederauferstandene Banker entdeckt, darunter Xenomorph, GoldDigger und SpyNote. Die Türkei, Spanien und Frankreich sind weiterhin die Hauptziele für Angreifer dieser Kategorie. Beliebte Mods für Messenger-Anwendungen wie Telegram, Signal und WhatsApp werden weiterhin für die Verbreitung von Spyware missbraucht. Darüber hinaus verbreitet sich SpyLoans weiterhin im PlayStore und stellt für gefährdete Opfer eine Erpressungsgefahr dar.

Zusammenfassend lässt sich sagen, dass das dritte Quartal 2023 ein beispielloses Ausmaß an Cyber-Bedrohungen offenbart hat. Der Anstieg der Bedrohungsaktivität während einer Saison, in der die Online-Präsenz normalerweise zurückgeht, gibt Anlass zur Sorge. Während wir uns der Wintersaison nähern, die traditionell von einer höheren Bedrohungslage geprägt ist, sind wir wachsam, um zu sehen, ob sich dieser Trend weiter verschärft.

Vielen Dank für Ihr anhaltendes Vertrauen in Avast. Bleiben Sie sicher und geschützt.

Jakub Křoustek, Malware-Forschungsdirektor

Methodik

Dieser Bericht ist in zwei Hauptabschnitte gegliedert: *Desktop-bezogene Bedrohungen ,* in denen wir unsere Informationen zu Angriffen beschreiben, die auf die Betriebssysteme Windows, Linux und Mac abzielen, mit besonderem Schwerpunkt auf webbezogenen Bedrohungen, und *Mobilgeräte-bezogene Bedrohungen ,* in denen wir Beschreiben Sie die Angriffe, die sich auf die Betriebssysteme Android und iOS konzentrieren.

Wir verwenden in diesem Bericht den Begriff „ *Risikoverhältnis“ ,* um die Schwere spezifischer Bedrohungen zu bezeichnen. Er wird als monatlicher Durchschnitt aus „Anzahl der angegriffenen Benutzer / Anzahl der aktiven Benutzer in einem bestimmten Land“ berechnet. Sofern nicht anders angegeben, sind berechnete Risiken nur für Länder mit mehr als 10.000 aktiven Benutzern pro Monat verfügbar.

Ein blockierter Angriff ist definiert als eine eindeutige Kombination aus dem geschützten Benutzer und einer blockierten Bedrohungskennung innerhalb des angegebenen Zeitraums.

In diesem Bedrohungsbericht haben wir mit einer detaillierteren Kennzeichnung verschiedener Betrugsbedrohungstypen begonnen, was im Vergleich zu den vorherigen Berichten zu einer separaten Verfolgung von z. B. Malvertising führte. Darüber hinaus haben wir einige weitere Bedrohungsdatenquellen hinzugefügt, um eine noch bessere Sichtbarkeit der Bedrohungslandschaft zu ermöglichen.

Besondere Geschichte: TikTok-Finanzbetrug: Eine eskalierende Bedrohung, die durch künstliche Intelligenz angeheizt wird

TikTok, bekannt für seine Viralität und die sich schnell verbreitenden digitalen Trends, hat sich zu einem fruchtbaren Boden für Finanzbetrug entwickelt, insbesondere für solche, die Kryptowährungen betreffen. Die große Reichweite der Plattform, gepaart mit ihrer Anziehungskraft auf ein jüngeres Publikum, stellt eine attraktive Perspektive für böswillige Akteure dar, die darauf abzielen, ahnungslose Benutzer auszunutzen.

Die Betrügereien agieren unter einer Fassade der Legitimität und werden oft mit einem Fake-Video einer seriösen Person eingeleitet, die eine Kryptowährungsbörse unterstützt. Benutzer werden dazu verleitet, sich an der angeblichen Börse anzumelden, indem sie einen Promo-Code verwenden, der ihrem Konto angeblich eine beträchtliche Menge Bitcoin gutschreibt. Beim Versuch, diese Gelder abzuheben, verlangt die Plattform jedoch eine vorläufige Überweisung von Bitcoin, um das Konto des Benutzers zu „verifizieren“. Ohne es zu wissen, stellen Opfer, die dieser Anforderung nachkommen, fest, dass nicht nur das versprochene Bitcoin unerreichbar ist, sondern auch, dass alle an die Plattform überwiesenen Gelder für die Cyberkriminellen, die den Betrug inszenieren, unwiederbringlich verloren sind.

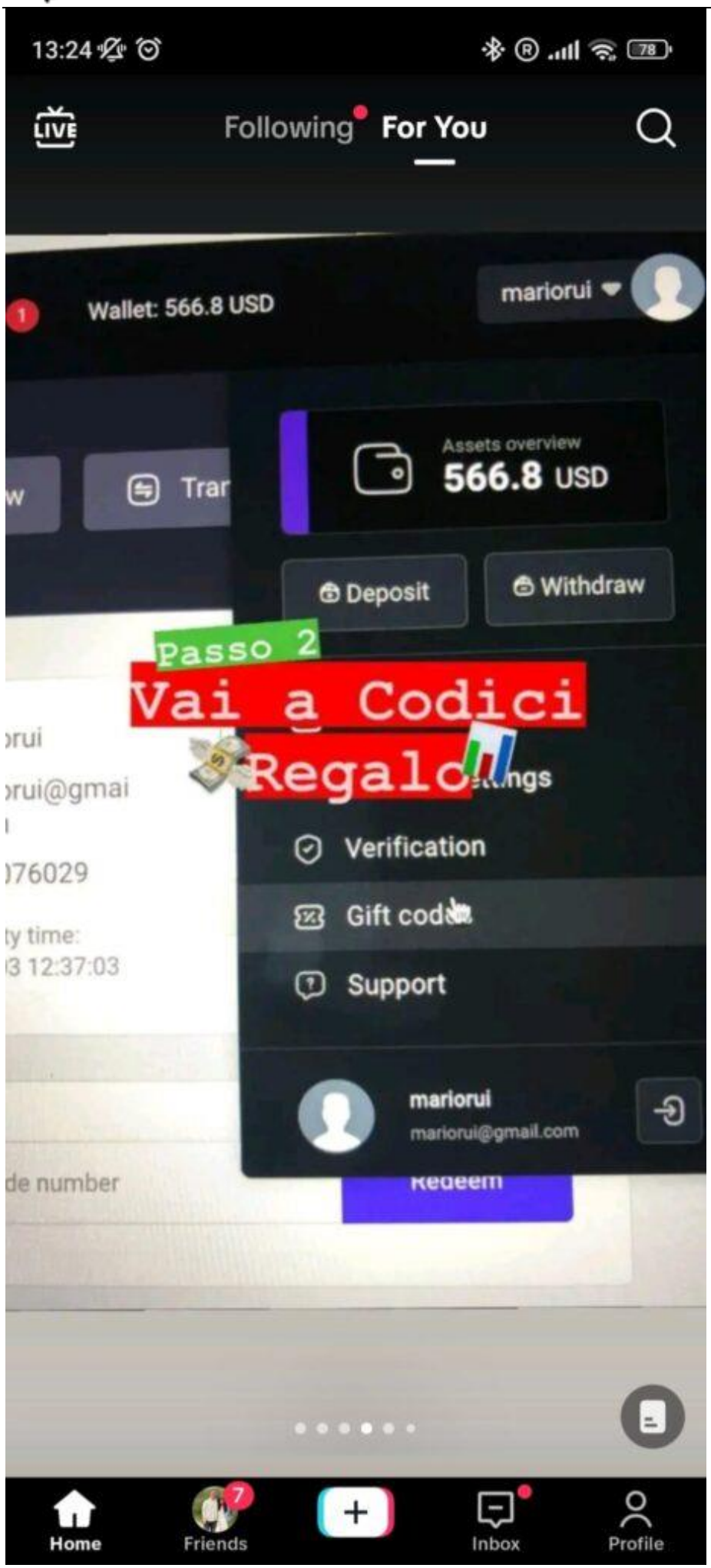
Im Mittelpunkt dieser Betrügereien steht der illegale Einsatz künstlicher Intelligenz (KI) zur Erstellung von Deepfake-Videos. Berüchtigte Persönlichkeiten wie Elon Musk, Mr. Beast, Sam Altman, Warren Buffet, Joe Rogan, Donald Trump und Tucker Carlson werden in betrügerischen Empfehlungen für Kryptowährungsbörsen imitiert. Diese gefälschten Empfehlungen locken Benutzer mit dem Versprechen erheblicher Bitcoin-Belohnungen und bereiten so den Boden für finanzielle Täuschung.

Beispiele von Videos, die auf TikTok im Umlauf sind und sich als Elon Musk und Donald Trump ausgeben

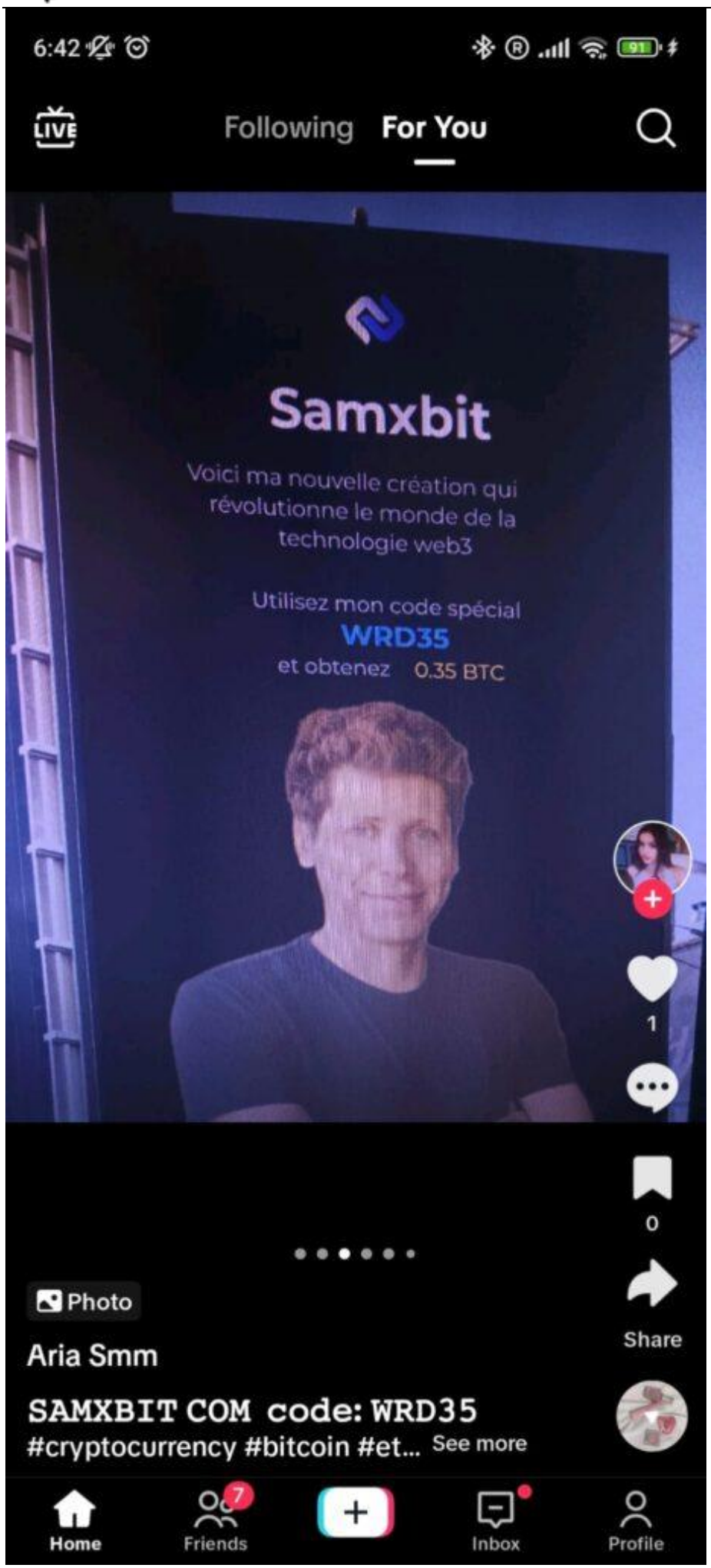
Der böswillige Einsatz von KI , insbesondere Deepfake-Technologie, unterstreicht die zunehmende Raffinesse von Cyber-Gegnern. Durch die Erstellung überzeugender gefälschter Videos seriöser Personen manipulieren Betrüger erfolgreich das Vertrauen der Öffentlichkeit. Diese Ausnutzung verdeutlicht nicht nur einen besorgniserregenden Trend zu Cyber-Bedrohungen auf Social-Media-Plattformen, sondern veranschaulicht auch das Potenzial von KI bei der Steigerung der Wirksamkeit von Finanzbetrug. Deepfake-Technologie, einst die Domäne hochqualifizierter Personen, wird immer zugänglicher, was es immer schwieriger macht, echte Empfehlungen von erfundenen zu unterscheiden.

Diese Betrügereien, die ursprünglich auf englischsprachige Zielgruppen beschränkt waren, haben sprachliche Barrieren überwunden und sind in nicht englischsprachige Regionen vorgedrungen. Jüngste Erscheinungsformen dieser Betrügereien wurden in verschiedenen Sprachen beobachtet, darunter Spanisch, Deutsch, Italienisch und Französisch, was auf eine zunehmende Bedrohungslandschaft hindeutet. Die mehrsprachige Ausbreitung dieser Betrügereien stellt eine globale Bedrohung dar und unterstreicht die Notwendigkeit einer multinationalen Zusammenarbeit bei der Bekämpfung dieser KI-gesteuerten Betrügereien.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55



DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55



Auf TikTok kursieren Screenshots von Betrugsvideos auf Italienisch und Französisch

Obwohl TikTok die primäre Bühne für diese Betrügereien ist, deuten die Beweise auf einen plattformübergreifenden Ansatz böswilliger Akteure hin. Auch Plattformen wie YouTube wurden zur Verbreitung betrügerischer Inhalte genutzt, was auf einen größeren digitalen Fußabdruck und eine größere Reichweite dieser betrügerischen Praktiken hindeutet. Allein TikTok hat monatlich mehr als 1 Milliarde aktive Nutzer, was den Oberflächenangriff riesig macht. Als wir begannen, den Zugriff auf diese Betrugswebsites zu blockieren, konnten wir innerhalb weniger Tage mehrere tausend Benutzer schützen.

Bei den TikTok-Betrügereien handelt es sich nicht um Einzelfälle, sondern vielmehr um Indikatoren für einen wachsenden Trend KI-gesteuerter Cyber-Bedrohungen. Die Leichtigkeit der Verbreitung von Fehlinformationen durch Deepfake-Technologie gepaart mit der Verlockung schneller finanzieller Gewinne ist eine wirkungsvolle Kombination, die den Weg für raffiniertere Betrügereien in der Zukunft ebnen könnte. Die potenziellen Auswirkungen reichen über den wirtschaftlichen Verlust einzelner Personen hinaus bis hin zu einem umfassenderen Vertrauensverlust in digitale Plattformen und namhafte Persönlichkeiten.

Luis Corrons, Sicherheitsevangelist

Desktop-bezogene Bedrohungen

Advanced Persistent Threats (APTs)

Ein Advanced Persistent Threat (APT) ist eine Art Cyberangriff, der von hochqualifizierten und entschlossenen Hackern durchgeführt wird, die über die Ressourcen und das Fachwissen verfügen, um in das Netzwerk eines Ziels einzudringen und eine langfristige Präsenz unentdeckt aufrechtzuerhalten.

APT-Gruppen missbrauchen zunehmend unvollständige Validierungsprozesse für den Erwerb einer Treibersignatur. Signierte Treiber, die in der Regel von seriösen Anbietern herausgegeben werden, gelten als sicher und für die Verwendung innerhalb eines Betriebssystems autorisiert. Durch die Untergrabung dieses Vertrauens umgehen APTs nicht nur Erkennungsmechanismen, sondern erhalten auch heimlichen und privilegierten Zugriff auf ein Zielsystem, wodurch herkömmliche Sicherheitsprotokolle praktisch überflüssig werden. Dieser gewagte Ansatz stellt die Grundlagen der Cybersicherheit in Frage und unterstreicht die Notwendigkeit kontinuierlicher Innovation und Wachsamkeit bei der Abwehr sich entwickelnder APT-Bedrohungen.

Anfang Juni 2023 entdeckten wir unbekannte signierte Treiber von Microsoft. Diese signierten Treiber wurden von der signierten Binärdatei NSecRTS.exe verteilt, die Shandong Anzai Information Technology Co., Ltd. zugeschrieben wird. Es ist erwähnenswert, dass NSecRTS als reguläre Überwachungssoftware anerkannt ist und vom QiAnXin Virus Response Center erwähnt wurde .

Darüber hinaus haben wir festgestellt, dass NSecRTS.exe einen von Microsoft signierten Treiber löscht. Bei einer umfassenden Untersuchung haben wir mehrere böswillige Aktivitäten im Zusammenhang mit diesem Treiber aufgedeckt. Eine davon war die Einschleusung von benutzerdefiniertem RAT in legitime Prozesse.

Unsere Beobachtungen führten uns dazu, Opfer auf den Philippinen und in Thailand zu identifizieren. Trotz der Sammlung umfangreicher Informationen konnten wir die Angriffe nicht eindeutig einer bestimmten Entität zuordnen.

Aktive geopolitische Konflikte ziehen aufgrund der volatilen und chaotischen Natur solcher Umgebungen häufig die Aufmerksamkeit von APTs auf sich. Diese oft staatlich geförderten und gut organisierten Gruppen sehen Konflikte als Chance, die Instabilität für ihre eigenen strategischen Ziele auszunutzen. Der Nebel des Krieges bietet einen bequemen Deckmantel für ihre Aktivitäten und ermöglicht es ihnen, das Chaos zur Durchsetzung ihrer politischen, wirtschaftlichen oder militärischen Ziele zu nutzen. Insbesondere haben die APTs weiterhin den anhaltenden Krieg in der Ukraine ausgenutzt, und weitere Konflikte, wie der in Berg-Karabach, sind auf ihrem Radar aufgetaucht.

Einer der beliebtesten Infektionsvektoren für die APT-Gruppen in diesem Quartal war CVE-2023-38831, eine Schwachstelle in WinRAR, die es einem Angreifer ermöglicht, beliebigen Code auf dem Rechner des Opfers auszuführen. In vielen Fällen erhalten Opfer ein Schadarchiv als Anhang einer Phishing-E-Mail. Beim Öffnen des Archivs mit einer anfälligen Version von WinRAR führt das Opfer unfreiwillig Schadcode aus, der zu einer Infektion des Computers führen kann. Wir könnten sehen, dass es von mehreren Bedrohungsakteuren missbraucht wird, einschließlich Angriffen auf ukrainische Regierungsinstitutionen, das Militär und Regierungen in Ländern wie Malaysia, Vietnam, den Philippinen und anderen.

Berüchtigte Unternehmen wie Lazarus, MustangPanda und APT41 führen ihre globalen Kampagnen unermüdlich fort, verfeinern ihre Taktiken kontinuierlich und erweitern ihr Malware-Arsenal. Diese Gruppen erforschen kontinuierlich neue Techniken, führen neue Tools ein und integrieren Sprachen wie Nim und Rust in ihre Toolkits.

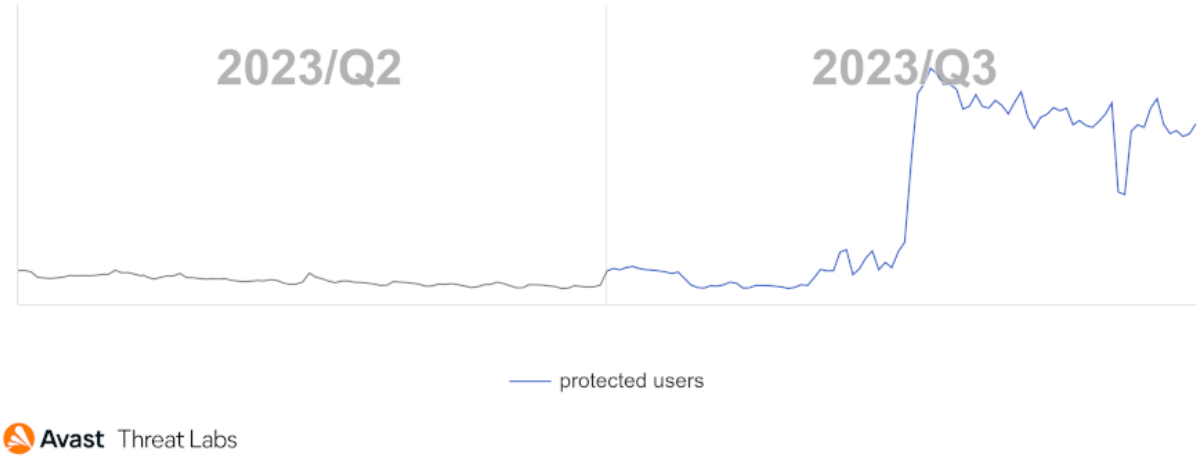
Luigino Camastra, Malware-Forscher
Igor Morgenstern, Malware Researcher

Adware

Adware gilt als unerwünscht, wenn sie ohne Zustimmung des Benutzers installiert wird, das Surfverhalten verfolgt, den Webverkehr umleitet oder persönliche Informationen für böswillige Zwecke wie Identitätsdiebstahl sammelt.

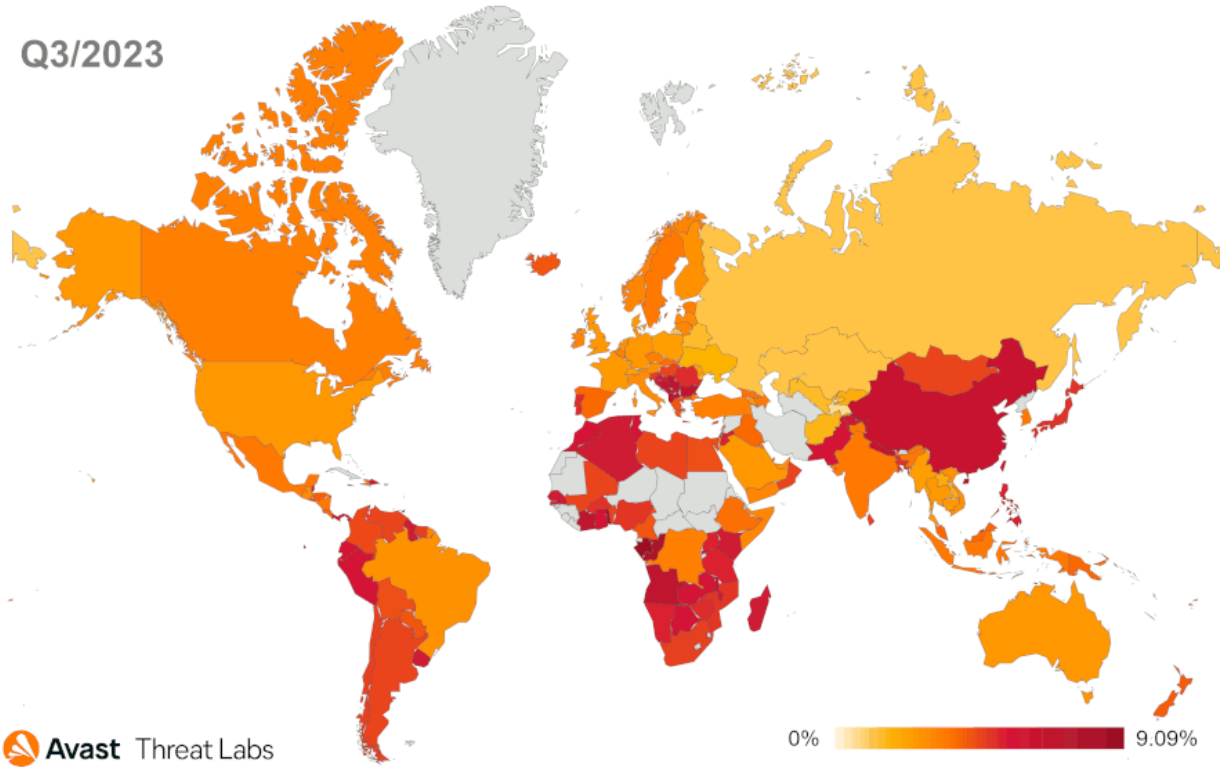
Adware erfreut sich aufgrund der Möglichkeiten der Monetarisierung und der Verbreitung potenziell unerwünschter Programme (PUP) und Malware immer größerer Beliebtheit. Obwohl die Verbreitung von Malware über Adware nicht die primäre Methode zur Infektion der Computer der Opfer ist, haben wir uns im dritten Quartal 2023 auf Adware-Erkennungen konzentriert, um diese potenzielle Bedrohung zu überwachen.

Die Ergebnisse genauerer Adware-Erkennungen sind in der folgenden Tabelle dargestellt. Dieses Quartil zeigt einen Anstieg der Adware-Aktivitäten, der durch die SocialBar-Adware verursacht wird.



Globales Avast-Risikoverhältnis durch Adware für Q2/2023 und Q3/2023

Die neuen Erkennungen helfen uns, einen globalen Überblick zu geben. Unsere Telemetrie meldet die vier aktivsten Regionen in Bezug auf Adware-Bedrohungen; nämlich Südamerika, Afrika, Südosteuropa und Ostasien. Siehe die Karte unten.



Karte mit dem globalen Risikoverhältnis für Adware im dritten Quartal 2023 und im zweiten Quartal 2023

Adware-Freigabe

Die neuen Nachweise reduzierten den Anteil unbekannter Stämme von 33 % auf 6 %. Die SocialBar ist im dritten Quartal 2023 mit 58 % der Adware-Marktführer. Die folgende Liste zeigt die am häufigsten verwendeten Ad-Server mit lustigen DNS-Einträgen:

- hissedassessmentmistake[.]com

- vertrauenswürdiger Turnstileboyfriend[.]com
- Happeningurinepomposity[.]com
- schändliches Vorwort[.]com
- Secondquaver[.]com
- usetalentedpunk[.]com
- Lyricsgrand[.]com

Der Rest der Anteile verteilt sich wie folgt auf andere Adware-Stämme:

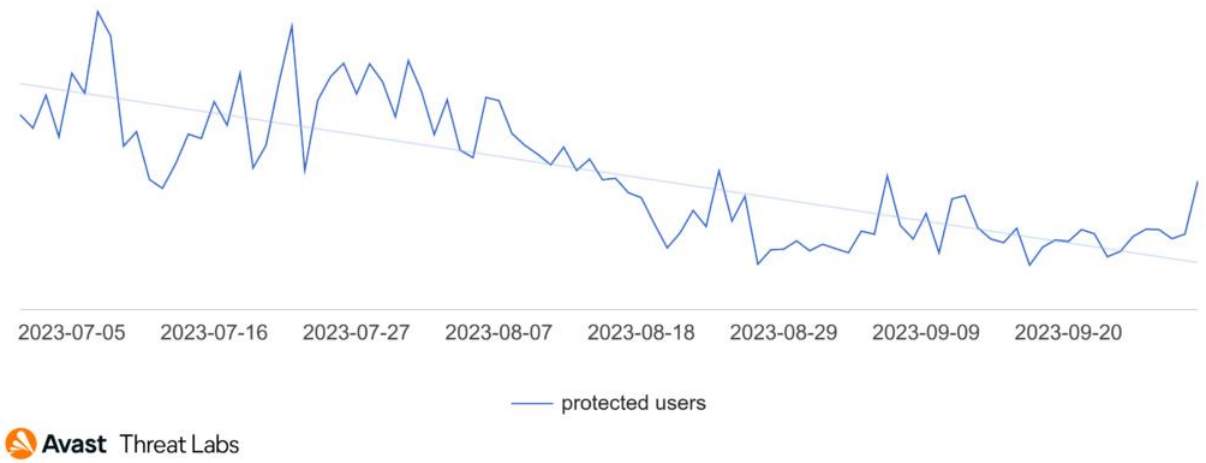
- SchlammOrange (7%)
- DealPly (3 %)
- Relevantes Wissen (2 %)
- Neoreklami (2%)
- MicroTag (2%)

Martin Chlumecký, Malware-Forscher

Bots

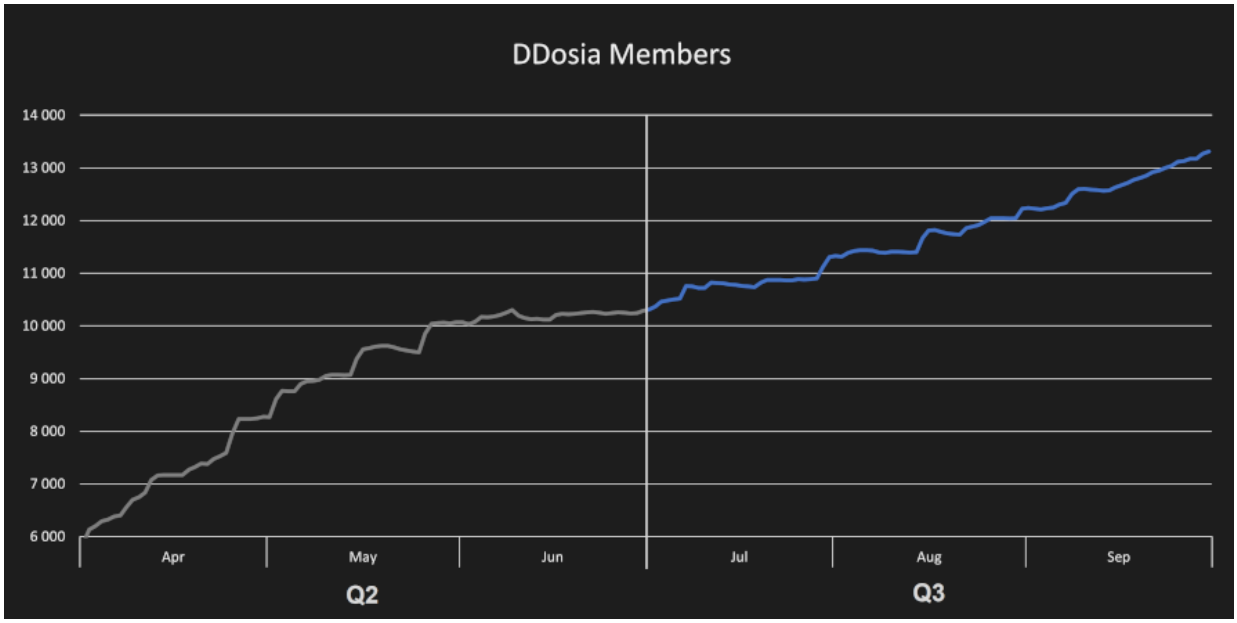
Bots sind Bedrohungen, die hauptsächlich daran interessiert sind, den langfristigen Zugriff auf Geräte zu sichern, um deren Ressourcen zu nutzen, sei es durch Fernsteuerung, Spam-Verteilung oder Denial-of-Service-Angriffe (DoS).

Die wahrscheinlich einschneidendste Veränderung in der Botnet-Landschaft ereignete sich Ende August – der vom FBI angeführte Versuch, das Qakbot-Botnet auszuschalten und zu zerschlagen. Interessanterweise war das Ziel nicht nur die Command-and-Control-Infrastruktur (C&C), sondern es wurde auch versucht, infizierte Clients vom Botnetz zu trennen, wodurch es effektiv schwieriger wurde, das Botnetz unter einer neuen Infrastruktur wiederzubeleben. Es ist bereits ein offensichtlicher Rückgang der Zahl der Kunden zu verzeichnen, die versucht wurden, für das Botnetz zu gewinnen, und zwar im August auf ein Fünftel des „normalen“ Wertes. Aus Botnet-Sicht sind dies zwar gute Nachrichten, die Spam-Versandfunktionen von Qakbot sind dadurch jedoch nicht beseitigt worden. Der mit der Verbreitung von Qakbot in Zusammenhang stehende Bedrohungsakteur (TA577) begann kurz nach der Abschaltung von Qakbot mit der Verbreitung von DarkGate als eine seiner Phishing-Payloads.



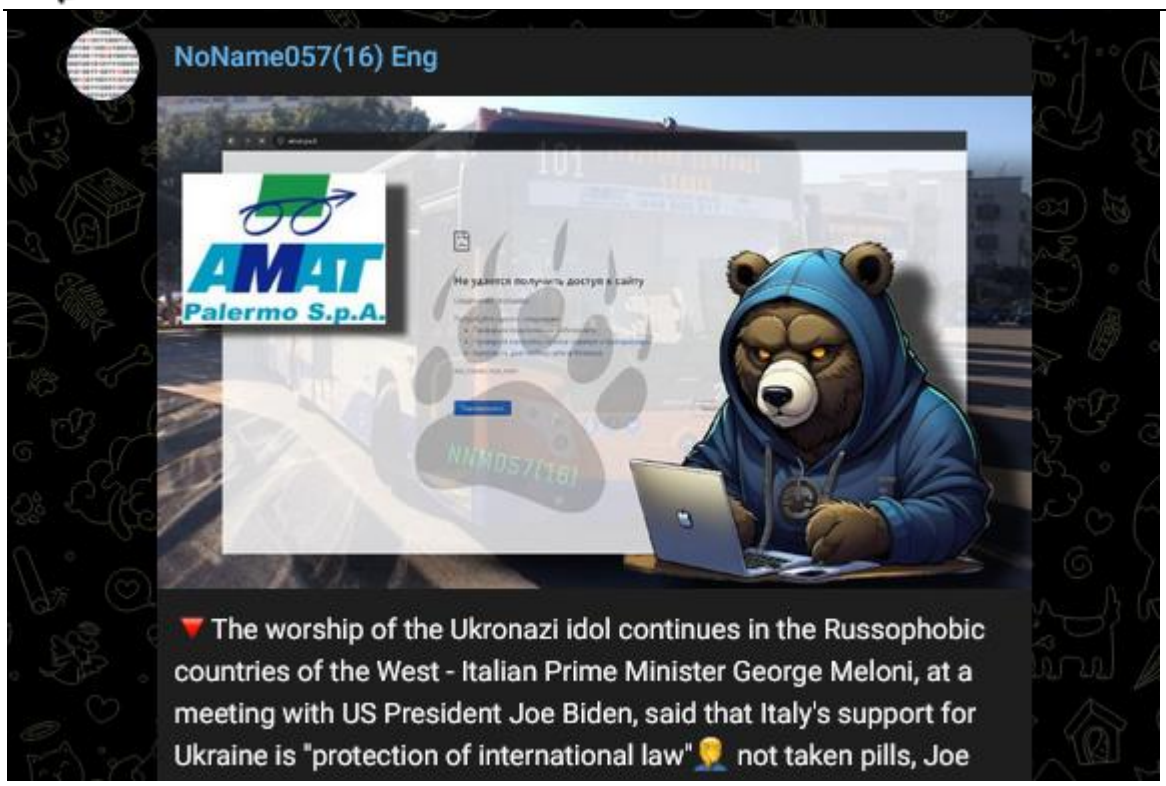
Anzahl der im dritten Quartal 2023 vor Qakbot geschützten Benutzer

Wir behalten die Bedrohungsgruppe NoName056(16) und ihr DDosia-Projekt im Auge. Bis Ende September überstieg die Mitgliederzahl 13.000 Nutzer. Basierend auf den Zahlen des Vorquartals gelang es ihnen, mit einem stetigen Zuwachs von etwa 1.000 Mitgliedern pro Monat etwas an Dynamik zu gewinnen. Ihre *Vorgehensweise* bleibt dieselbe – DDoS-Angriffe, Vorwürfe der Russophobie und Prahlerei mit ihren Erfolgen. Es ist ziemlich bedauerlich, dass die Verwendung irreführender Terminologie durch die Mainstream-Medien, wie etwa die fälschliche Bezeichnung von DDoS-Angriffen als Hacks oder die Bezeichnung ihrer Täter als Hacker, manchmal unabsichtlich die öffentliche Wahrnehmung solcher Angriffe aufbläht und den Tätern den gewünschten Auftrieb in der Medienberichterstattung verschafft. Dies gilt insbesondere für Internet-Aktivistengruppen, bei denen die Berichterstattung in den Medien auch das Ansehen der Gruppe in der Community steigert und so ihr potenzielles Rekrutierungspotenzial weiter steigert.



Anzahl der DDosia-Mitglieder im Jahr 2023

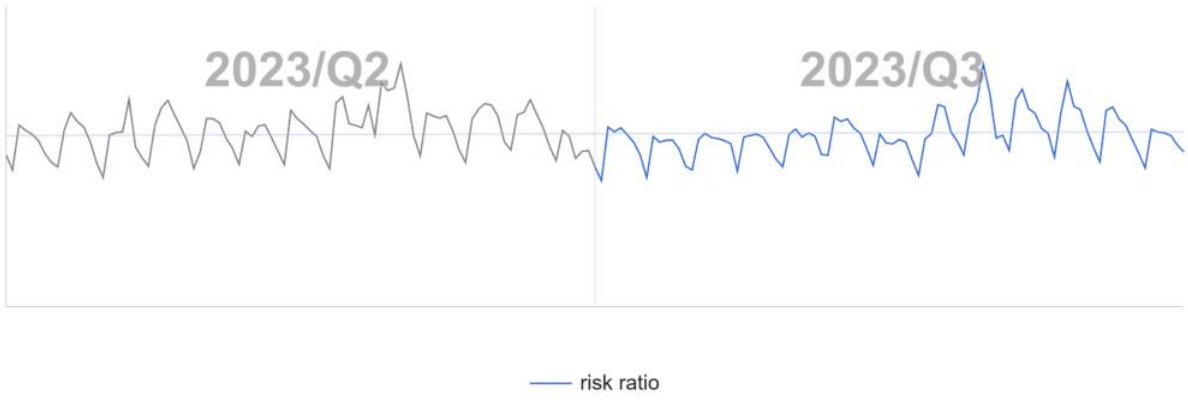
Bei den Zielen handelte es sich bei den meisten anvisierten Top-Level-Domains (TLDs) um . *pl* (Polen, 15 %), . *lt* (Litauen, 11 %) und . *es* (Italien, 9%). Die beiden erstgenannten sind keine schockierende Überraschung, da es in diesen Regionen aktive Verwicklungen in den Ukraine-Russland-Konflikt gibt. Im Falle Italiens schien die Gruppe auf das Treffen von Joe Biden mit der italienischen Premierministerin Giorgia Meloni zu reagieren.



Kommentar von NoName057(16) zum Treffen von Joe Biden mit der italienischen Premierministerin Georgia Meloni

Finanzinstitute waren in diesem Quartal das häufigste Ziel, vermutlich aufgrund des potenziellen finanziellen Schadens und der Chance auf eine deutlich bessere Berichterstattung in der Presse. Nebenbei bemerkt: Sie scheinen mit Foto- und Grafikstilen zu experimentieren. Sie begannen damit zu experimentieren, ein Foto eines Bären durch ein Cartoon-Bild eines Bären zu ersetzen, der als Kapuzenpullover stilisiert war (31). st Juli) oder Angehöriger einer Armee (ab Ende September).

Trotz der Abschaltung des Qakbot ist die globale Risikoquote leicht gestiegen – teils aufgrund der Tatsache, dass es in der Mitte des Quartals geschah, teils aufgrund der erhöhten Aktivität anderer Botnets. Wir haben einen deutlichen Anstieg der Aktivität der Botnetze Tofsee (+41 %), Emotet (+25 %) und Trickbot (+13 %) festgestellt. Was andere Familien betrifft, so deuten unsere Telemetriedaten auf einen Rückgang bei den meisten anderen Familien hin.



Avast Threat Labs

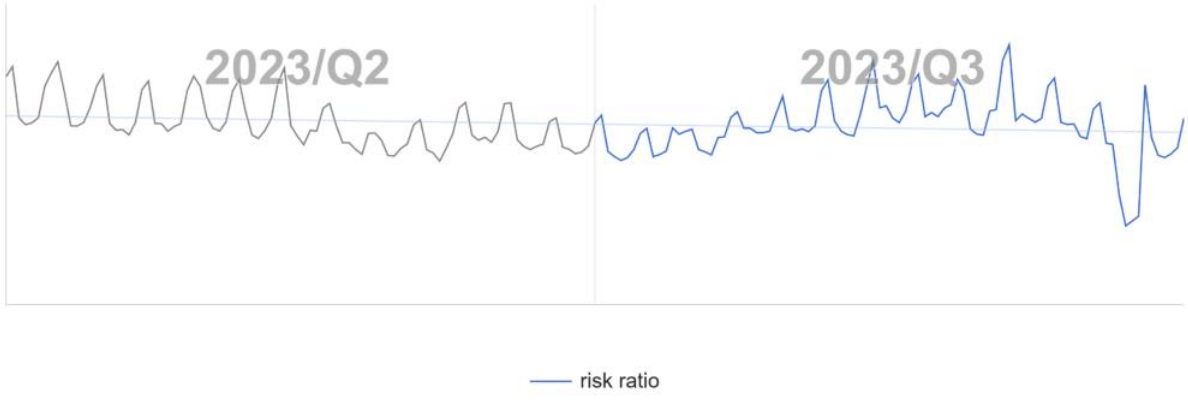
Globales Risikoverhältnis in der Benutzerbasis von Avast in Bezug auf Bots im dritten Quartal 2023

Adolf Streda, Malware-Forscher

Coinminer

Coinminer sind Programme, die die Hardwareressourcen eines Geräts nutzen, um Kryptowährungstransaktionen zu verifizieren und als Entschädigung Kryptowährungen zu verdienen. In der Welt der Malware kapern Coinminer jedoch stillschweigend die Computerressourcen eines Opfers, um Kryptowährungen für einen Angreifer zu generieren. Unabhängig davon, ob es sich bei einem Coinminer um einen legitimen oder um Schadsoftware handelt, ist es wichtig, unsere Richtlinien zu befolgen .

Im Vergleich zum letzten Quartal beobachteten wir im dritten Quartal 2023 einen weiteren Rückgang des Risikoverhältnisses im Coinmining-Bereich um 4 %. Dies ist ein anhaltender Abwärtstrend bei Coinmining-Bedrohungen.

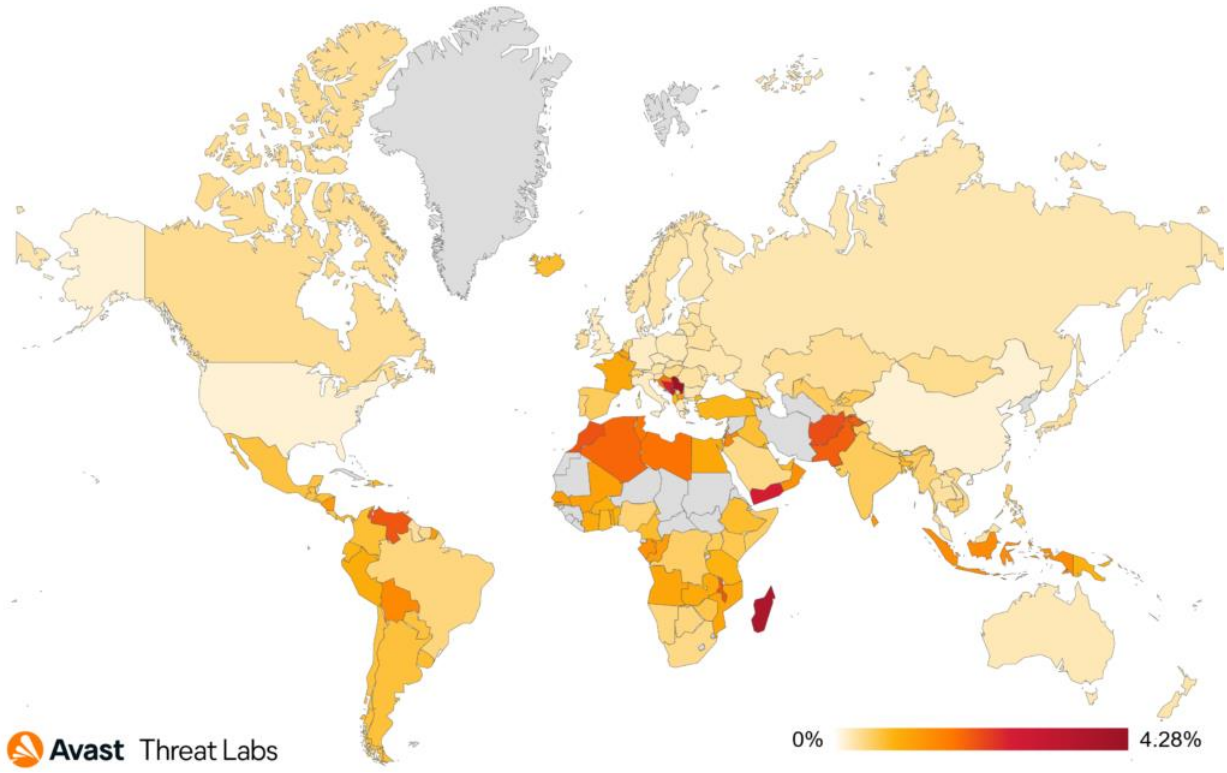


Avast Threat Labs

Globales Risikoverhältnis in der Benutzerbasis von Avast in Bezug auf Coinminer im dritten Quartal 2023

Im dritten Quartal 2023 waren Benutzer in Serbien erneut dem höchsten Risiko ausgesetzt, einem Coinminer zu begegnen, ein regionaler Trend, den wir in den letzten Quartalen beobachten konnten. Bei einer Risikoquote von 4,28 % bedeutet dies jedoch einen

Risikorückgang um 26 % und einen Rekordtiefstand. Eine ähnliche Situation ist in anderen Ländern mit höherem Risiko zu beobachten, darunter Madagaskar mit einer Risikoquote von 3,73 %, Montenegro mit einer Risikoquote von 3,29 % und Bosnien und Herzegowina mit einer Risikoquote von 2,64 %.



Globale Risikoquote für Informationsdiebe im dritten Quartal 2023

Leider stieg der Marktanteil von XMRig, wo wir einen Anstieg von 30 % verzeichneten und nun 23,65 % des gesamten Coinmining-Marktanteils ausmachen. Auch CoinBitMiner wurde immer beliebter und steigerte seinen Malware-Marktanteil um 10 %, was einem Marktanteil von 2,02 % entspricht. Andere Web-Miner verzeichneten einen leichten Rückgang um 5 % und kommen nun zusammen auf einen Marktanteil von 61,46 %. Andere Stämme wie FakeKMSminer, VMiner und CoinHelper verzeichneten mit 27 %, 62 % bzw. 29 % einen recht starken Rückgang der Aktivität.

Die häufigsten Coinminer mit ihrem Marktanteil im zweiten Quartal 2023 waren:

- Web-Miner (61,46 %)
- XMRig (23,65 %)
- CoinBitMiner (2,02 %)
- FakeKMSminer (1,58 %)
- NeoScrypt (1,03 %)
- CoinHelper (0,77 %)
- VMiner (0,73 %)

Jan Rubin, Malware-Forscher

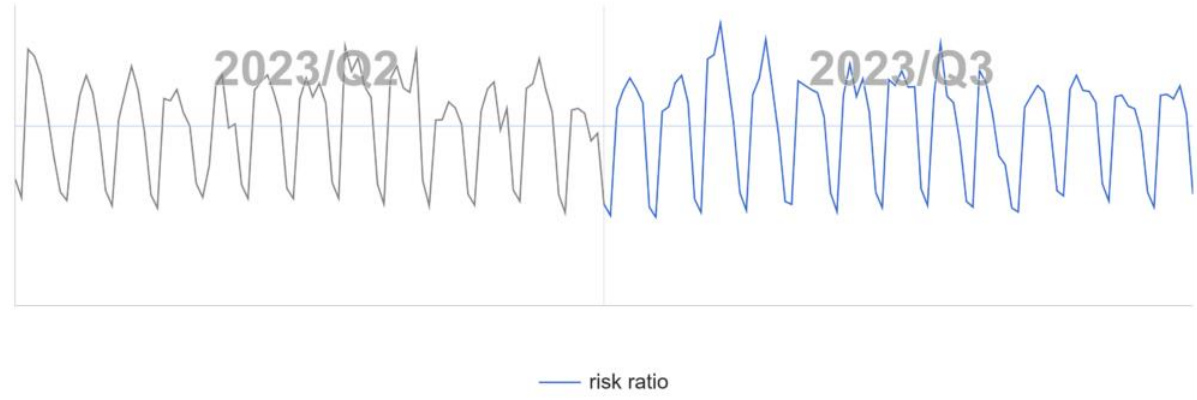
Informationsdiebe

Informationsdiebe stehlen ausschließlich Wertgegenstände vom Gerät des Opfers. Typischerweise konzentrieren sie sich auf gespeicherte Anmeldeinformationen, Kryptowährungen, Browsersitzungen/Cookies, Browserkennwörter und private Dokumente.

Die weit verbreitete Meinung, dass „ich nichts zu verbergen habe und meine Daten nicht schützen muss“, ist grundsätzlich falsch. Sogar Personen, die glauben, dass ihre Daten keinen Wert haben, könnten feststellen, dass im großen Maßstab alles wertvoll werden kann. Diese Art von Daten können durch Verkäufe in Untergrundforen monetarisiert, für weitere Angriffe, einschließlich gezielterer Betrügereien und Phishing (sogenanntes *Spear-Phishing*), genutzt, für Erpressungen genutzt werden und vieles mehr. Bleibt sicher da draußen.

Im dritten Quartal 2023 beobachteten wir im Vergleich zum Vorquartal einen Rückgang der Aktivität von Informationsdiebstahlern um insgesamt 6 %, was den kürzlich beobachteten rückläufigen Trend verlangsamte.

Die größte Veränderung in diesem Quartal besteht darin, dass Raccoon Stealer unseren Daten zufolge in diesem Quartal einen enormen Aktivitätsrückgang mit einem Rückgang des Marktanteils um 72 % verzeichnete. Andererseits steigerten einige andere Sorten ihre Präsenz deutlich, nämlich AgentTesla, Fareit und SnakeKeylogger, was für einen Ausgleich sorgte.

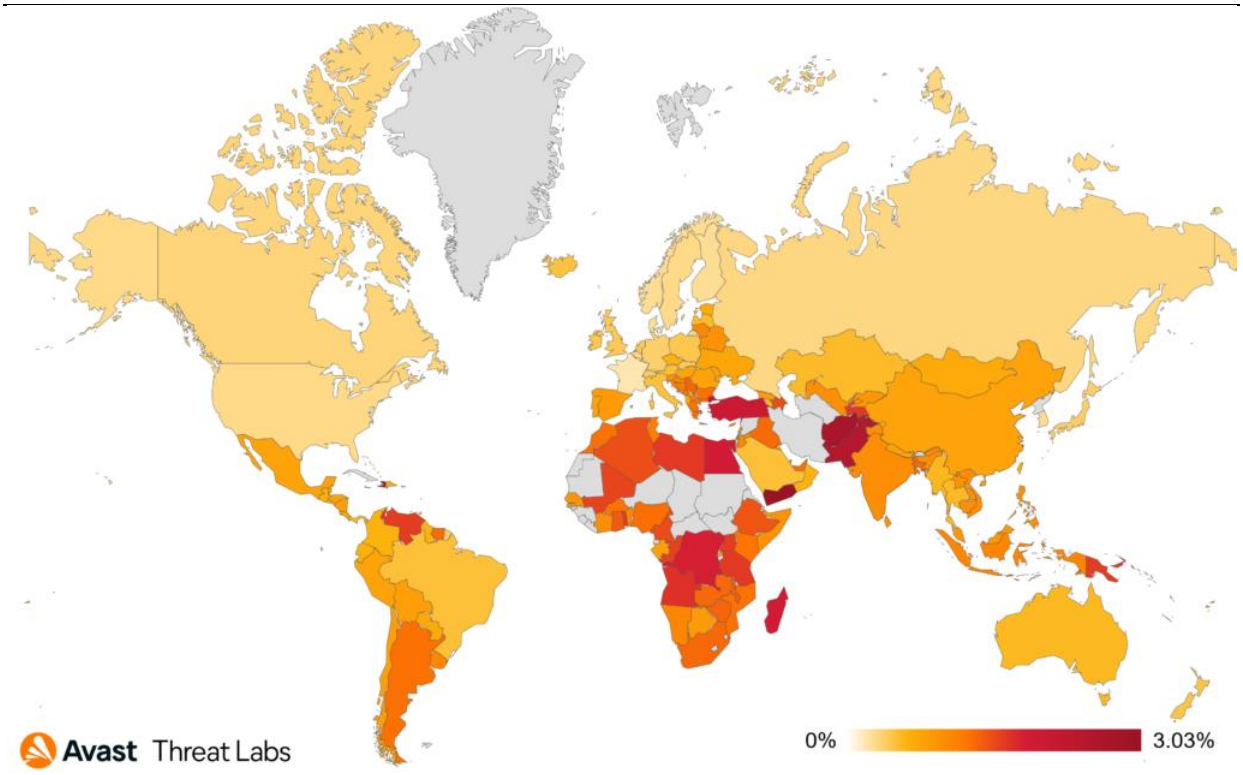


Avast Threat Labs

Globales Risikoverhältnis in der Avast-Benutzerbasis in Bezug auf Informationsdiebstahler im dritten Quartal 2023

Die geografische Verteilung blieb zwischen Q2 und Q3/2023 konstant. Länder, in denen wir eine größere Nutzerbasis mit der höchsten Risikoquote haben, sind Pakistan (2,47 %), die Türkei (2,05 %) und Ägypten (1,90 %). Erfreulicherweise sank die Risikoquote in diesen Ländern im Vergleich zum Vorquartal um 5 %, 7 % bzw. 14 %.

Den größten Anstieg der Risikoquote in Bezug auf Informationsdiebstahl verzeichneten die Ukraine (44 %), die Vereinigten Staaten (21 %) und Indien (16 %).



AgentTesla hält und unterstreicht weiterhin den ersten Platz unter den beliebtesten Informationsdiebstahlern und steigert seinen Marktanteil weiter um 9 %. FormBook, der Zweitplatzierte, blieb konstant und steigerte seinen Marktanteil lediglich um 0,55 %. Fareit, SnakeKeylogger und Stealc verzeichneten alle einen Anstieg ihres Marktanteils um 11 %, 68 % bzw. 4 %.

Glücklicherweise war Raccoon Stealer mit seinem Marktanteilsrückgang von 72 % nicht allein. RedLine und Arkei waren im dritten Quartal 2023 hinsichtlich ihres Marktanteils jeweils 10 % weniger aktiv, während ViperSoftX um weitere 7 % zurückging.

Die häufigsten Informationsdiebe mit ihrem Marktanteil im dritten Quartal 2023 waren:

- AgentTesla (29,14 %)
- FormBook (11,39 %)
- RedLine (5,46 %)
- Fareit (5,45 %)
- Lokibot (4,51 %)
- Arkei (3,96 %)
- ViperSoftX (2,08 %)
- Waschbärendieb (1,95 %)

Erwähnenswert sind auch neue Informationsdiebe bzw. deren Varianten, die in den letzten Monaten einen deutlichen Anstieg ihrer Aktivität verzeichneten. Diese böswilligen Akteure entwickeln ihre Taktiken ständig weiter, um Sicherheitsmaßnahmen zu umgehen und sensible Daten herauszufiltern. Dazu gehören häufig neue Techniken, die Schwachstellen sowohl in der Software als auch im menschlichen Verhalten ausnutzen. Daher ist es für Organisationen und Einzelpersonen unerlässlich, wachsam zu bleiben und robuste Cybersicherheitsstrategien zu übernehmen, um ihre wertvollen Informationen zu schützen.

Es wurde festgestellt, dass die neue Version von Rilide Stealer, die auf Bankdaten abzielt, mit Google Chrome Manifest V3 funktioniert . Eine der neuen Funktionen des Manifest V3 ist die Deaktivierung der Remotecodeausführung in Browsererweiterungen. Um dieses Problem zu umgehen, verwendet Rilide Stealer Inline-Ereignisse zusammen mit Declarative Net Requests-Regeln, um den Code remote auszuführen und die Header der Content Security Policy zu entfernen. Da Rilide mithilfe lokaler Loader auf den infizierten Computern verteilt wird, also ohne Verwendung des Chrome Web Store, ist kein Überprüfungsprozess erforderlich, der diese Vorgehensweise aufdecken würde.

Darüber hinaus wurden neue Verbindungen zwischen Rhadamanthys und dem Hidden Bee-Coinminer entdeckt , die neue Einblicke in das Innenleben und Implementierungsdetails liefern. Eine andere Malware namens DarkGate ist ein Loader mit weiteren Funktionen wie Keylogging, Kryptowährungs-Mining, Diebstahl von Informationen aus Browsern und einer umfassenden Fernzugriffsfunktionalität. Auch wenn die Malware bereits einige Jahre zurückverfolgt werden kann, befindet sie sich immer noch in aktiver Entwicklung und führt neue Vektoren ein, um Opfer zu infizieren, beispielsweise über Microsoft Teams.

Darüber hinaus erfreut sich auch Lumma, ein Malware-as-a-Service-Stealer, immer größerer Beliebtheit. Die Fähigkeiten der Malware reichen vom Kryptowährungsdiebstahl bis hin zum Angriff auf Browsererweiterungen mit Zwei-Faktor-Authentifizierung (2FA), dem Sammeln von Bankdaten, Anmeldeinformationen und mehr.

Clipper sind im Allgemeinen kleine Schadprogramme, die dazu dienen, den Inhalt der Zwischenablage des Opfers gegen vom Angreifer angegebene Inhalte auszutauschen – in diesem Fall Krypto-Wallet-Adressen. Solche Clipper, die in den vergangenen Monaten an Popularität gewonnen haben, sind unter anderem Atlas Clipper, Keyzetsu Clipper und KWN Clipper , die in der Regel Telegram für die Befehls- und Kontrollkommunikation und Kaufangebote nutzen.

Jan Rubin, Malware-Forscher

Ransomware

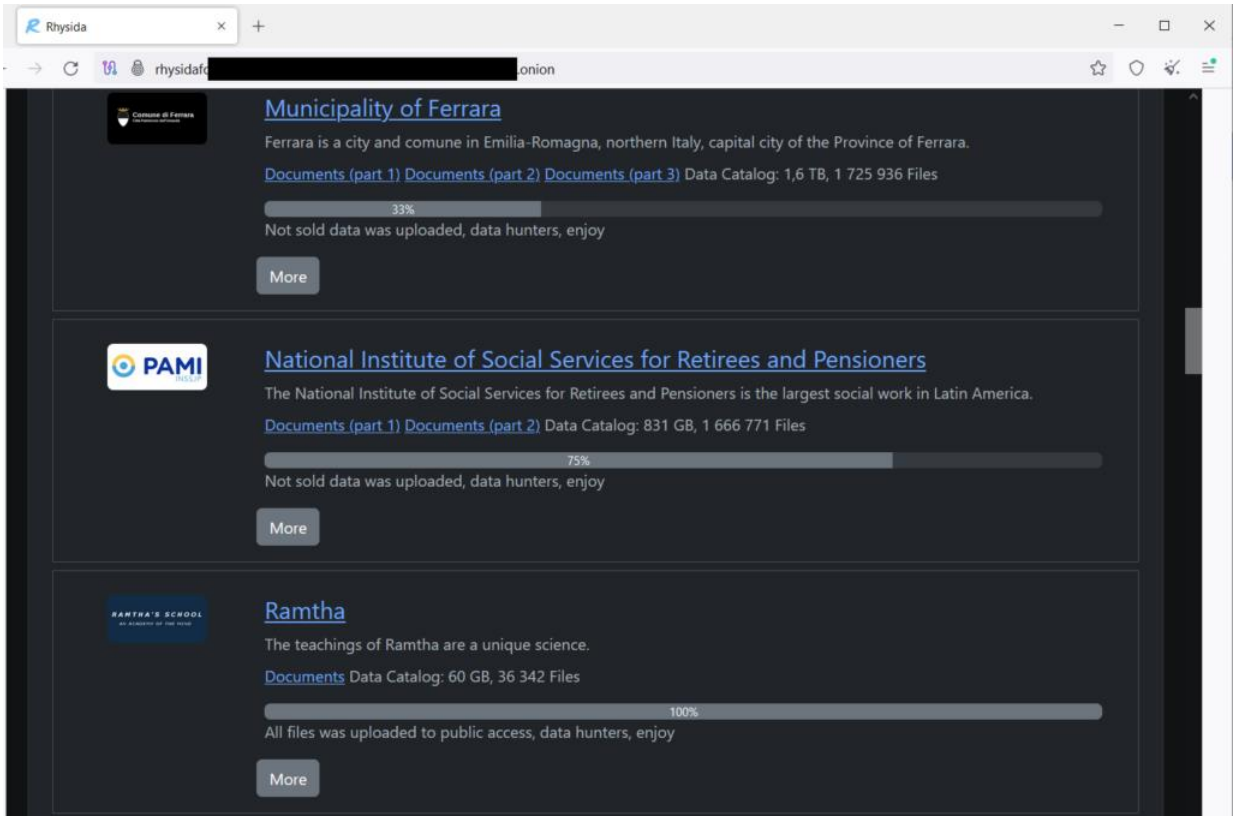
Ransomware ist jede Art von erpressender Schadsoftware. Der häufigste Untertyp verschlüsselt Dokumente, Fotos, Videos, Datenbanken und andere Dateien auf dem PC des Opfers. Diese Dateien werden unbrauchbar, ohne sie vorher zu entschlüsseln. Um die Dateien zu entschlüsseln, verlangen Angreifer Geld, „Lösegeld“, daher der Begriff Ransomware.

Die Verbreitung von Ransomware nimmt sicherlich nicht ab. Tatsächlich ist es das Gegenteil. Laut den Untersuchungen von Chainalysis beläuft sich der Gesamtbetrag der im ersten Halbjahr 2023 erpressten Gelder auf etwa 450 Millionen US-Dollar (im Vergleich zu 280 Millionen US-Dollar im ersten Halbjahr 2022). Dies ist auf eine Änderung der Taktik der Ransomware-Betreiber zurückzuführen – sie zielen tendenziell auf größere Opfer ab, was die Möglichkeit höherer Lösegeldbeträge mit sich bringt. Der durchschnittliche Zahlungsbetrag für die Top-Varianten beträgt bis zu 1,7 Millionen US-Dollar (Cl0p-Ransomware) und 1,5 Millionen US-Dollar (BlackCat-Ransomware).

Schwachstellen in beliebten Drittanbieteranwendungen, die in Unternehmen weit verbreitet sind, erleichtern Angreifern die Arbeit. haben wir über die SQL-Injection-Schwachstelle in der Übertragungssoftware Progress MOVEit geschrieben Im vorherigen Bedrohungsbericht .

Neben der Verschlüsselung der Opferdaten betreiben Ransomware-Banden zunehmend auch Datenerpressungen. Die Datenverschlüsselung kann gelöst werden, wenn das Unternehmen über eine gute Datensicherungsrichtlinie verfügt. Unabhängig davon kann die Datenerpressung und die anschließende Offenlegung interner Dokumente ein Problem darstellen. Bedenken Sie außerdem, dass bei Zahlung des Lösegelds das Versprechen, die erpressten Daten zu löschen, nicht immer eingehalten wird .

Einer der neuen Ransomware-Stämme, die in diesem Quartal auftauchten, war Rhysida. Die erste Erwähnung der Ransomware erfolgte im Mai 2023 und die Ransomware-Leak-Site listet bereits etwa fünfzig erfolgreich angegriffene Organisationen auf – Regierung, Gesundheitswesen, IT, Kommunen.



Rhysida-Leckseite im Dark Web

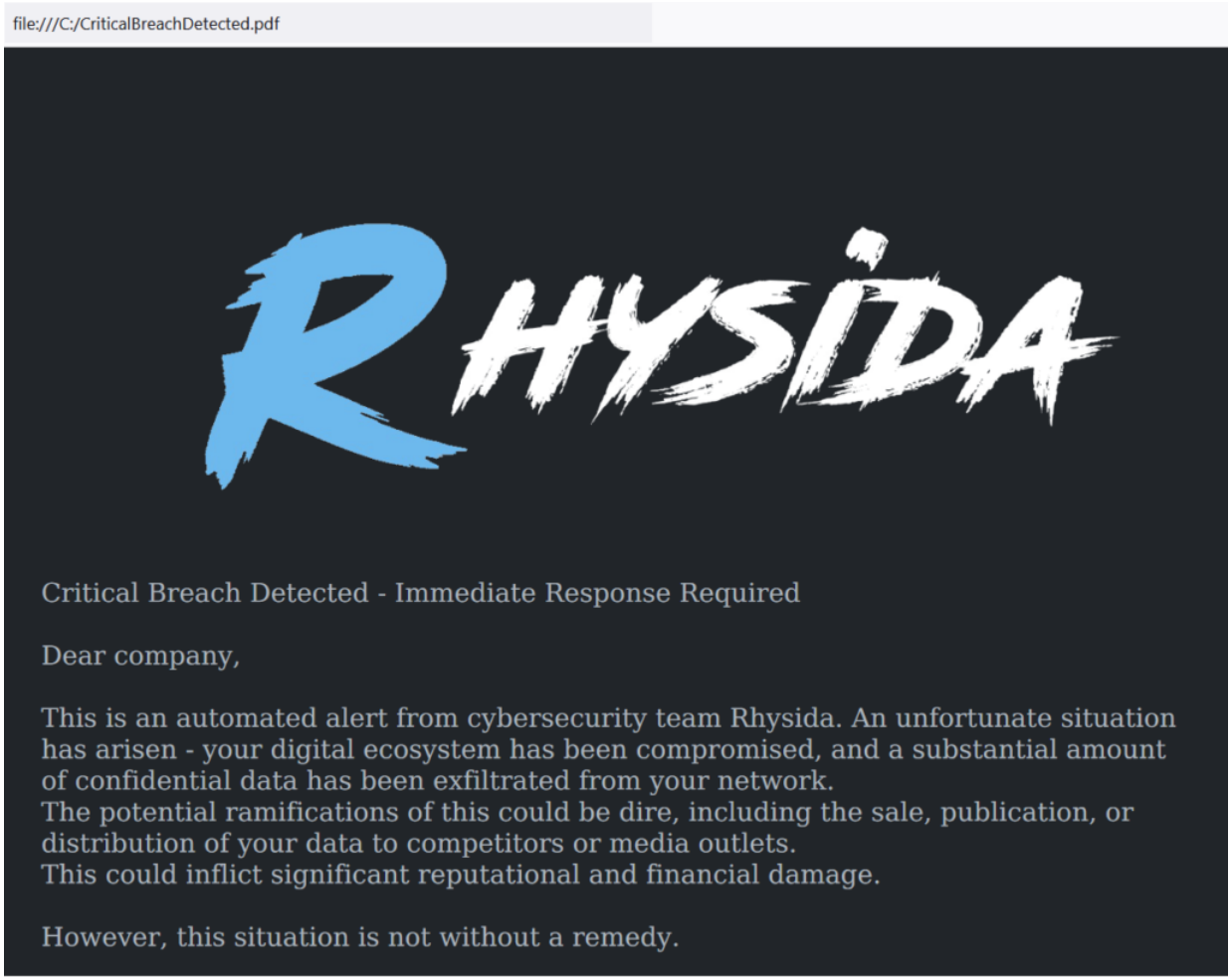
Der von der Rhysida-Bande verwendete Verschlüsselungscode ist eine 32-Bit- oder 64-Bit-EXE-Datei, die mit MinGW/GCC 6.3.0 kompiliert und mit GNU Linker 2.30 verknüpft wurde. Für kryptografische Operationen wird LibTomCrypt v 1.18.1 als Kryptobibliothek verwendet. Dateien werden durch AES-Verschlüsselung im Zählermodus verschlüsselt, der Dateischlüssel und IV werden durch RSA-4096 mit OAEP-Padding verschlüsselt.

Rhysida möchte bei der Dateiverschlüsselung so schnell wie möglich sein:

- **Intermittierende Datenverschlüsselung** . Nicht alles ist verschlüsselt. Bei größeren Dateien verschlüsselt Rhysida nur wenige unterschiedliche Dateiblöcke.
- **Multithread-Verschlüsselung** . Für jeden Prozessor hat Rhysida einen Verschlüsselungsthread erstellt. Während des Verschlüsselungsvorgangs sind alle Prozessoren im PC ausgelastet.

Aufgrund der Verwendung der *pthreads*- Bibliothek gehen wir davon aus, dass die Autoren der Rhysida-Ransomware einen Verschlüsseler entwickeln wollten, der auch leicht auf andere Plattformen portierbar ist.

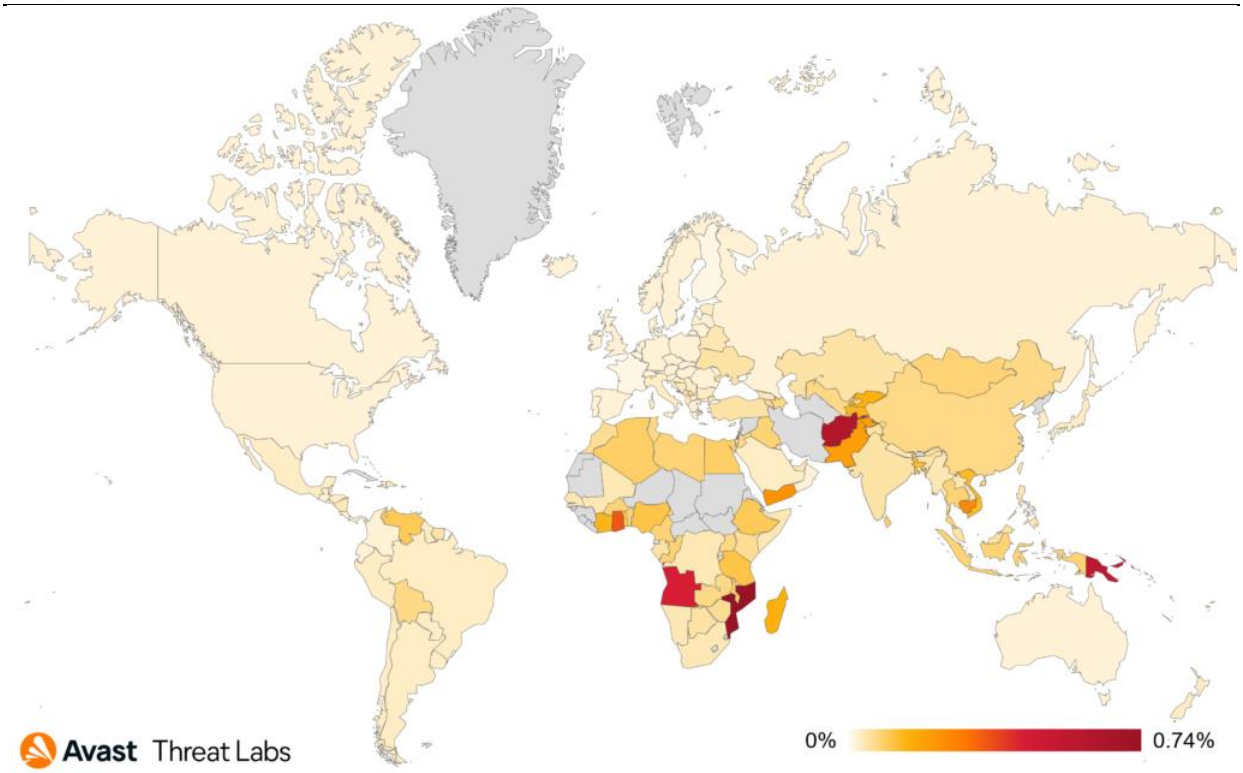
Rhysida legt in jedem Ordner eine Lösegeldforderungsdatei mit dem Namen „CriticalBreachDetected.pdf“ ab. Das folgende Bild zeigt ein Beispiel der Lösegeldforderung:



Inhalt des von Rhysida erstellten Lösegeldscheins

Weitere Informationen zu dieser Ransomware-Variante finden Sie in unserem Blogbeitrag .

Wie in jedem Thread-Bericht üblich, bringen wir einen Überblick über das Risikoverhältnis in unsere Benutzerbasis. Das folgende Bild zeigt die riskantesten Länder (in Bezug auf Ransomware).



Ransomware-Risikoverhältnis für Q3/2023

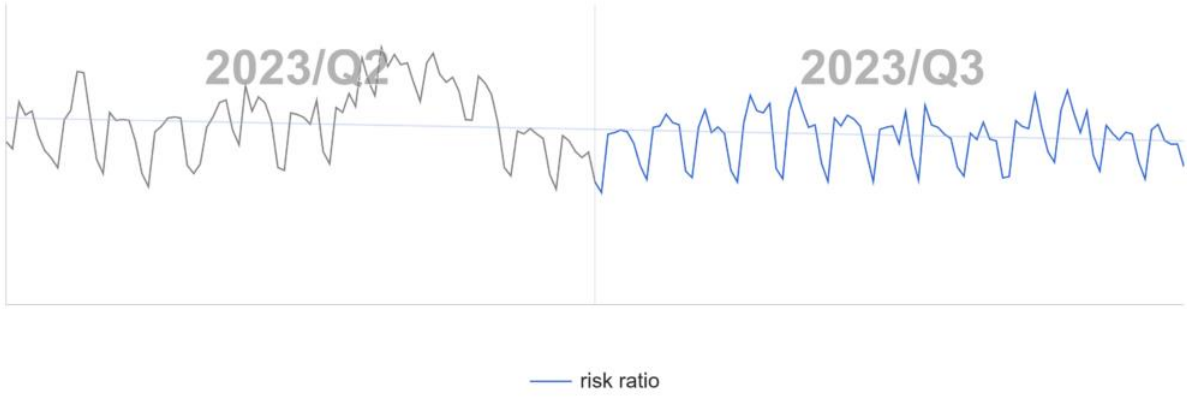
Die Liste der Länder, in denen das Risiko von Ransomware-Angriffen am höchsten ist:

- Mosambik (0,74 %)
- Angola (0,44 %)
- Ghana (0,35 %)
- Pakistan (0,20 %)

Die häufigsten Ransomware-Stämme, die wir gesehen und vor denen wir uns geschützt haben, finden Sie in der folgenden Liste:

- WannaCry (19 % des Ransomware-Anteils)
- STOP (15 %)
- Thanatos (3%)
- Zielunternehmen (2 %)
- LockBit (2%)
- Kryptonit (2%)
- Rätsel (1%)

Das Gesamtrisikoverhältnis unserer Nutzerbasis bleibt ungefähr gleich:



Avast Threat Labs

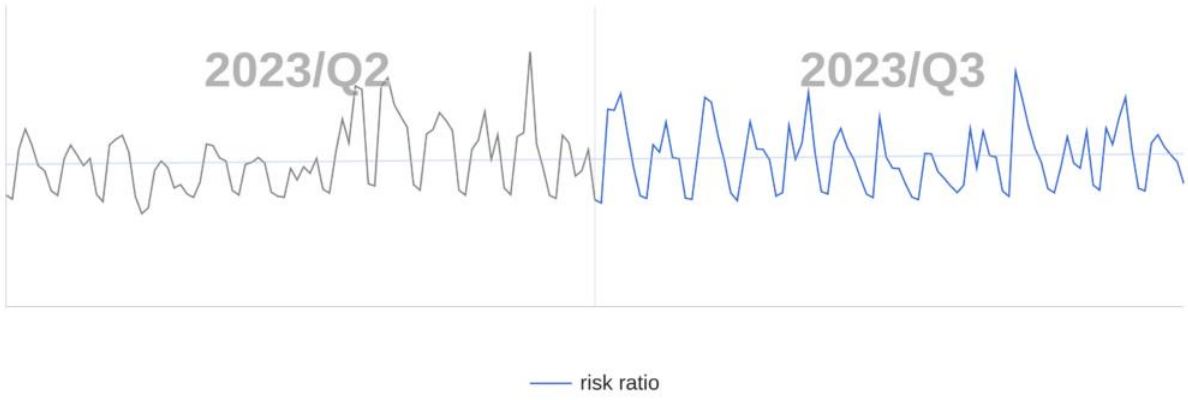
Entwicklung der Ransomware-Bedrohungen in unserer Benutzerbasis

Ladislav Zezula, Malware- Forscher
Jakub Křoustek, Malware-Forschungsdirektor

Remote-Access-Trojaner (RATs)

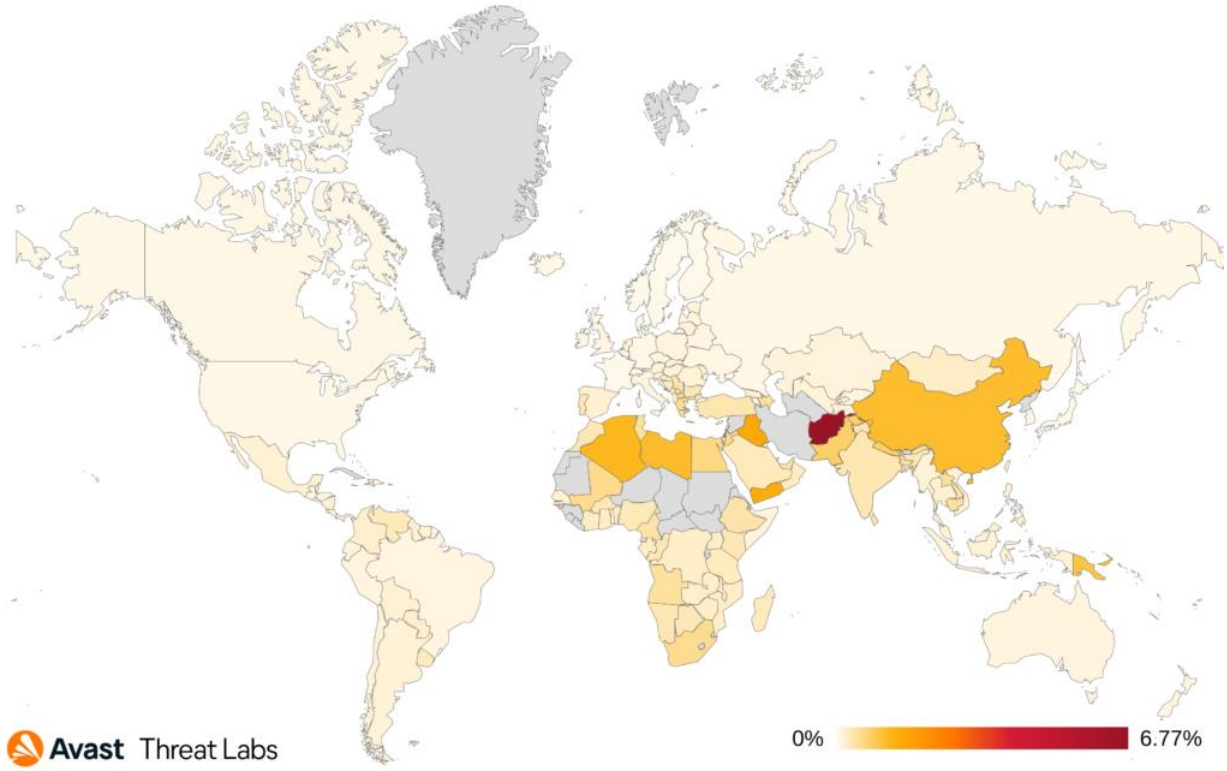
Ein Remote Access Trojaner (RAT) ist eine Art bösartiger Software, die es Unbefugten ermöglicht, Fernkontrolle über den Computer oder das Gerät eines Opfers zu erlangen. RATs werden typischerweise durch Social-Engineering-Techniken verbreitet, beispielsweise durch Phishing-E-Mails oder das Herunterladen infizierter Dateien. Nach der Installation gewähren RATs dem Angreifer vollständigen Zugriff auf das Gerät des Opfers und ermöglichen ihm so die Durchführung verschiedener böswilliger Aktivitäten wie Spionage, Datendiebstahl, Fernüberwachung und sogar die Übernahme der Kontrolle über die Webcam und das Mikrofon des Opfers.

Der im zweiten Quartal 2023 beobachtete wachsende Trend der RATs setzt sich im dritten Quartal 2023 fort. Insgesamt sehen wir einen leichten Anstieg der Risikoquote. Der erhebliche Anstieg von Remcos, den wir im ersten und zweiten Quartal 2023 gemeldet haben, scheint sich verlangsamt zu haben, wobei die Zahlen von Remcos in etwa auf dem gleichen Niveau wie im Vorquartal bleiben. Wir beobachten jedoch ein stetiges Wachstum des DBatLoader-Droppers, der neben anderen Nutzlasten auch Remcos liefern kann.



Globales Risikoverhältnis in der Benutzerbasis von Avast in Bezug auf RATs im dritten Quartal 2023

Die Länder mit der höchsten Risikoquote in Bezug auf RATs sind wie üblich Afghanistan, Irak und Jemen, da HWorm in diesen Ländern ein wurmartiges Verhalten zu haben scheint, das weit verbreitet zu sein scheint. Darüber hinaus sehen wir njRAT auch im Irak und im Jemen recht aktiv. Länder mit dem größten Anstieg der Risikoquote sind Portugal (148 % Anstieg), Polen (55 %) und die Slowakei (43 %), verursacht durch Remcos und im Fall der Slowakei auch Warzone. Der stärkste Rückgang der Risikoquote wurde in Tschechien (42 % Rückgang), Belgien (34 %) und Japan (33 %) beobachtet. Dies hängt wiederum wahrscheinlich mit der Aktivität (oder im Moment der Abwesenheit) von Remcos und Warzone in diesen Ländern zusammen.



Karte, die das globale Risikoverhältnis für RATs im dritten Quartal 2023 zeigt

Der größte Anstieg des Marktanteils und der Anzahl geschützter Benutzer unter den am weitesten verbreiteten RATs im dritten Quartal 2023 geht auf NanoCore zurück. Beide Zahlen stiegen um nahezu 100 %. Griechenland, die Türkei und Ungarn sind am stärksten von dieser RAT bedroht, wir haben auch einen erheblichen Anstieg in Brasilien, Mexiko und Spanien beobachtet.

Einen noch größeren Anstieg verzeichnete XWorm, das um mehr als 400 % zulegte. Allerdings ist XWorm in der Gesamtzahl nicht so weit verbreitet, dass es in die Top-10-Liste gelangt wäre.

Warzone und AsyncRat verzeichneten den größten Rückgang des Risikoverhältnisses unter den am weitesten verbreiteten RATs, die wir sehen. Laut unseren Daten ging Warzone um 27 % und AsyncRat um 14 % zurück.

Die in unserer Nutzerbasis am weitesten verbreiteten Fernzugriffs-Trojanerstämme sind:

- HWurm
- Remcos
- njRAT
- AsyncRat
- Kriegsgebiet
- NanoCore
- QuasarRAT
- Gh0stCringe
- DarkComet
- Bifrost

Das Threat Research-Team von Uptycs entdeckte einen neuen RAT namens QwixxRAT, der erstmals Anfang August bemerkt wurde. Der QwixxRAT verfügt über einen ziemlich standardmäßigen Satz an Funktionen, darunter Keylogging, Informationsdiebstahl (Kreditkarten, Browserverlauf und Lesezeichen, Steam-bezogene Daten usw.), Spionage (Webcam, Mikrofon), das Ausführen von Befehlen auf infizierten Systemen und mehr. Es nutzt Telegram als C&C-Kanal.

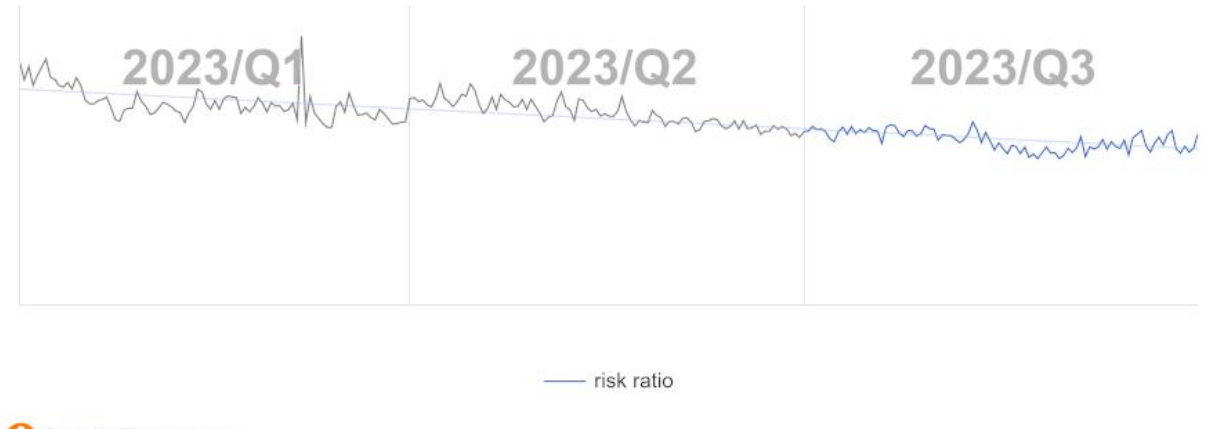
ZenRAT ist ein weiteres RAT, das im dritten Quartal 2023 erschien und von Proofpoint Emerging Threats gemeldet wurde . Es wurde festgestellt, dass dieser RAT mit dem legitimen Passwort-Manager Bitwarden auf der Website bitwariden[.]com gebündelt ist. Den Untersuchungen zufolge ist ZenRAT modular aufgebaut, laut Proofpoint wurde jedoch nur ein Modul gesehen, das offenbar Systeminformationen sammelt.

Ondřej Mokoš, Malware-Forscher

Rootkits

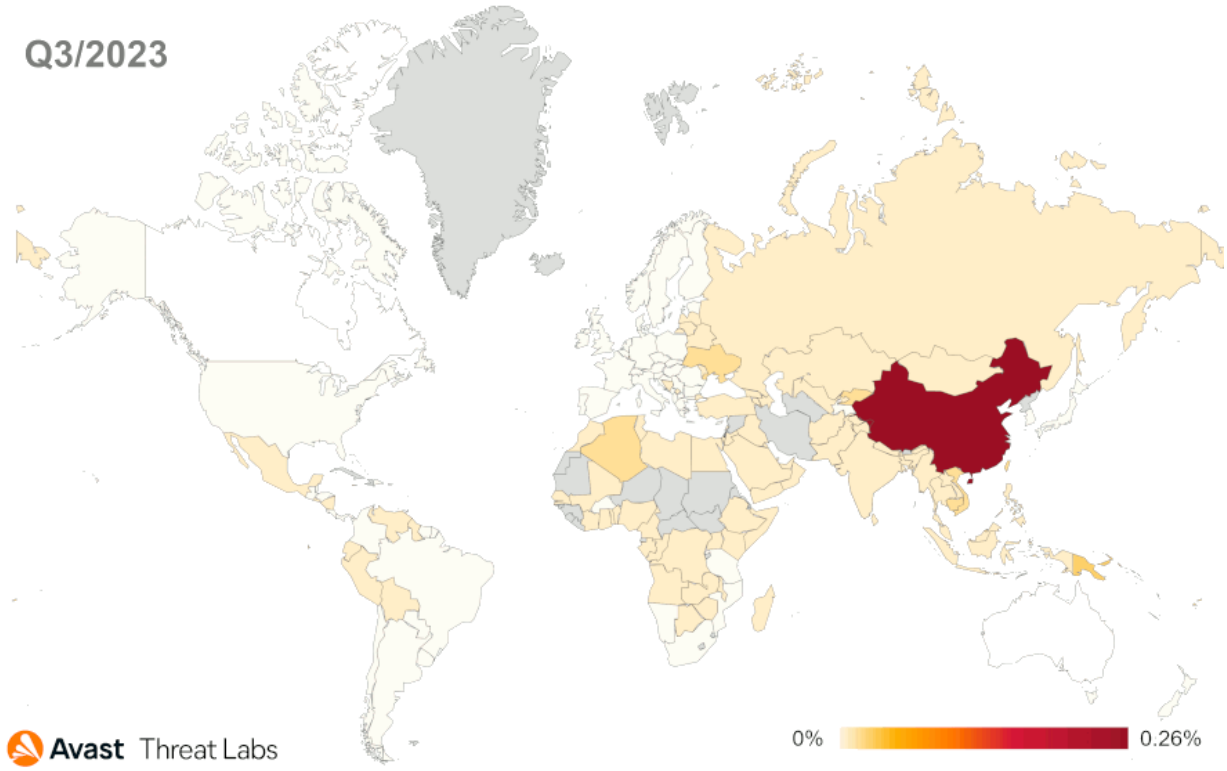
Rootkits sind bösartige Software, die speziell dafür entwickelt wurde, sich unbefugten Zugriff auf ein System zu verschaffen und hochgradige Berechtigungen zu erlangen. Rootkits können auf der Kernel-Ebene eines Systems agieren, was ihnen weitreichenden Zugriff und Kontrolle gewährt, einschließlich der Möglichkeit, kritische Kernel-Strukturen zu ändern. Dies könnte es anderer Malware ermöglichen, das Systemverhalten zu manipulieren und der Erkennung zu entgehen.

Der Trend der Rootkit-Aktivität ist seit Jahresbeginn stabil. Wir können auch feststellen, dass es weiterhin einen langfristigen Abwärtstrend gibt. Die folgende Grafik zeigt die Rootkit-Aktivität für die letzten drei Quartale.



Rootkit-Risikoverhältnis im 1. Quartal 2023 – 3. Quartal 2023

Bei der Betrachtung des Risikoverhältnisses für einzelne Länder behauptet China seine Spitzenposition hinsichtlich des Ausmaßes der Rootkit-Aktivitäten. Obwohl wir weltweit einen Rückgang der Aktivität beobachten, konnten wir einen besonderen Anstieg in der Ukraine (62 %) und in der Russischen Föderation (62 %) beobachten, insbesondere den Aktivitätsanstieg des R77RK-Rootkits.



Global risk ratio for rootkits in Q2 and Q3 2023

In September 2023, an updated version of R77Rootkit (1.5.0) was released, simplifying its deployment on victims' machines. However, there was no increase in the activity of this rootkit

despite the improvements. So, the R77RK is still the malware market leader with the same share (18%) as in the previous quarter.

Around 17% of unidentified strain rootkits are also in the market share, serving as kernel proxies for various activities involving elevated system privileges, such as terminating processes, altering network communications, and registry operations, among others. Compared to the previous quarter, an interesting feature is the increased use of the VMProtect to obfuscate driver functionality.

The third rootkit with the third-largest market share is the Pucmeloun rootkit, whose primary functionality is the modification of network traffic to redirect to different pages. It is a part of other adware that controls web requests on the kernel layer. Adware websites have primarily Chinese content.

The following is the comprehensive list of distinctly recognized Windows rootkit strains, along with their respective market shares:

- R77Rootkit (18%)
- Pucmeloun (13%)
- Alureon (7%)
- Cerbu (6%)
- Perkesh (6%)

In terms of Linux kernel rootkits, inspired by Syslogk, the threat actors continue hiding command line backdoors (or bots, depending on how the attacker controls the infected computers) with kernel rootkits that execute those via magic packets (e.g. AntiUnhide rootkit). We continue monitoring Linux kernel rootkits that reuse the code of open-source projects. For instance, Rocke reuses the code of Reptile Reptile and hides a secret protected shell that can be spawned via magic packets. and hides a secret protected shell that can be spawned via magic packets.

Martin Chlumecký, Malware Researcher
David Álvarez, Malware Analyst

Vulnerabilities and Exploits

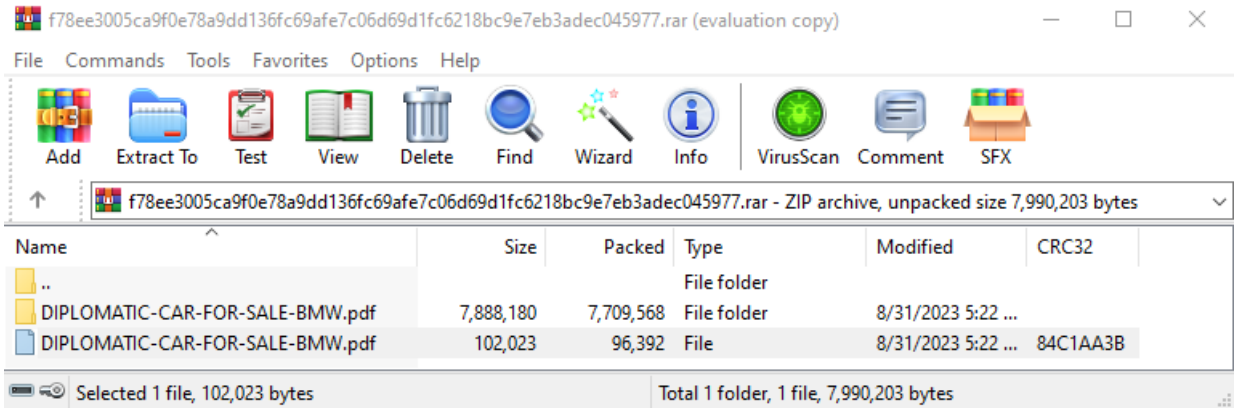
Exploits take advantage of flaws in legitimate software to perform actions that should not be allowed. They are typically categorized into remote code execution (RCE) exploits, which allow attackers to infect another machine, and local privilege escalation (LPE) exploits, which allow attackers to take more control of a partially infected machine.

WinRAR is not a frequent target of exploits, aside from the occasional path traversals. Our attention was therefore immediately captivated when we first heard about CVE-2023-38831, an easy-to-exploit WinRAR vulnerability, which allows an attacker to craft a malicious archive so that it contains both a benign lure (e.g., an image file) and a malicious payload. When an unsuspecting victim opens such a malicious archive in a vulnerable version of WinRAR and double clicks the lure file, the malicious payload will get executed instead. This is because opening files from inside WinRAR is internally implemented by extracting the target files into a temporary folder and then calling ShellExecute on them. Unfortunately, due to a buggy path normalization, it was possible to redirect the ShellExecute call to target a different file than the

one the user clicked on. For a more in-depth look at the exploit, we recommend reading this SecureLayer7 analysis.

This vulnerability was exploited as a zero-day in financially motivated attacks since at least April 2023. The attacks took place on trading forums and consisted of attackers posting exploit archives promising details of novel trading strategies. However, instead of exciting new trading strategies, the archives were used to spread the DarkMe malware (or the Guloader -> Remcos duo in some attacks). This campaign was initially discovered in July by the Group-IB Threat Intelligence unit. After reporting the vulnerability to RARLAB, a patched version of WinRAR was released in August.

Since WinRAR must be updated manually by downloading and installing the patched version, we can expect there will continue to be many users with unpatched versions in the future. While the exploit does require a fair amount of user interaction (not every targeted user will open the archive in WinRAR and double click the lure file), it is quite easy to craft an exploit archive (there is even a public PoC builder on GitHub), so it is likely that there will be threat actors experimenting with this vulnerability. And indeed, just recently Google TAG reported on "multiple government-backed hacking groups" exploiting this vulnerability. Let us therefore use this opportunity to remind the reader not to delay applying the update.



An exploit archive opened in a vulnerable version of WinRAR. Double-clicking the PDF file here would execute a malicious batch file located in the folder of the same name. Note that the PDF file does not have its usual icon. This is because there is an extra space appended to the end of the ".pdf" extension.

In other news, Google's Threat Analysis Group and Citizen Lab discovered a new in-the-wild zero-day exploit chain for iPhones. This chain started with a WebKit RCE (CVE-2023-41993) which was combined with a signature bypass (CVE-2023-41991) and ultimately ended with a kernel LPE (CVE-2023-41992). Post-exploitation, the chain deployed the Predator implant, known to be developed by the commercial spyware vendor Intellexa. The attackers also used a parallel exploit chain for Android devices, but unfortunately the full details of this chain remain unknown at the time.

As reported by Citizen Lab, one of the targets was former Egyptian MP Ahmed Eltantawy who announced his run for president in 2024. He was targeted through a man-in-the-middle (MitM) injection on plaintext HTTP, through a middlebox located at an ISP-level privileged network position. This essentially allowed the attackers to use a browser exploit with no user interaction required, similarly to how a watering hole or malvertising attack would work. While it is extremely hard to defend against such government-backed attackers, using a secure VPN

should mitigate the risk of ISP-level MitM injection. However, note that just a single HTTP request outside the VPN tunnel is all the attackers would need to still be able to inject the exploit.

Finally, in Q3/2023 the BLASTPASS exploit chain that was actively used by the infamous NSO Group to compromise fully patched iPhones in a zero-click manner. BLASTPASS was discovered by the Citizen Lab, who found it while helping check the device of a potential mercenary spyware victim. The initial memory corruption vulnerability appears to go by three different CVEs (CVE-2023-41064, CVE-2023-4863, and CVE-2023-5129), as there was some confusion at first about who should actually assign the CVE. Nevertheless, the vulnerable code is located in libwebp, Google's image rendering library for the WebP format. While this library is very widely used, it is not currently clear what conditions are needed for the vulnerability to be exploitable. There has been some great research into the root cause of the vulnerability and a public PoC to trigger a heap overflow. However, weaponizing this heap overflow seems like an absurdly difficult feat, so at least for the moment, we do not have to fear this vulnerability being exploited in the wild by less sophisticated attackers.

Jan Vojtěšek, Malware Reseracher

Web Threats

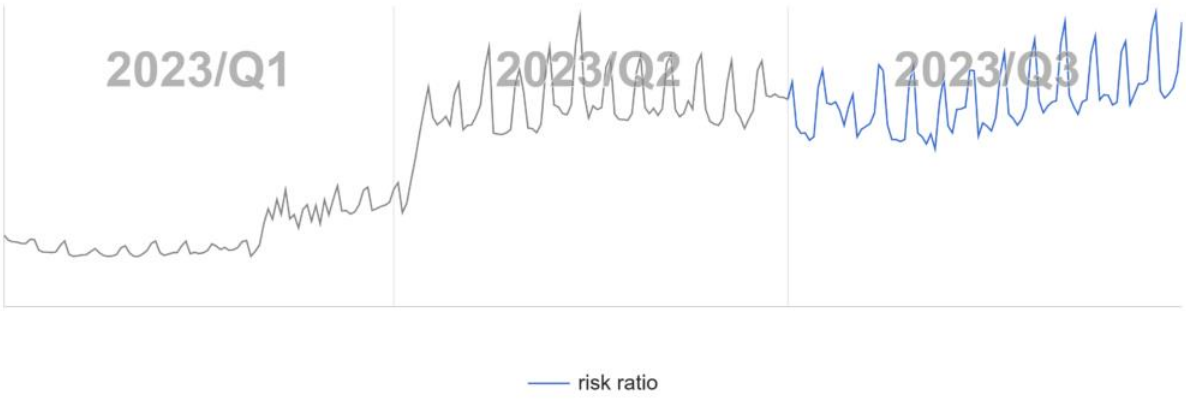
Users increasingly depend on the internet in their daily lives, exposing themselves to a growing array of potential risks, like stealing their personal data or financial losses. The rise in activities such as variations of financial scams, dating scams, fake push notifications and phishing threats in general underscores this trend.

The third quarter of 2023 was a growing quarter for web threats in general. Many types of threats started their growth at the end of the holiday season and this growth only continued in the third quarter. But there are also some exceptions. Let us take a closer look at them.

Scams

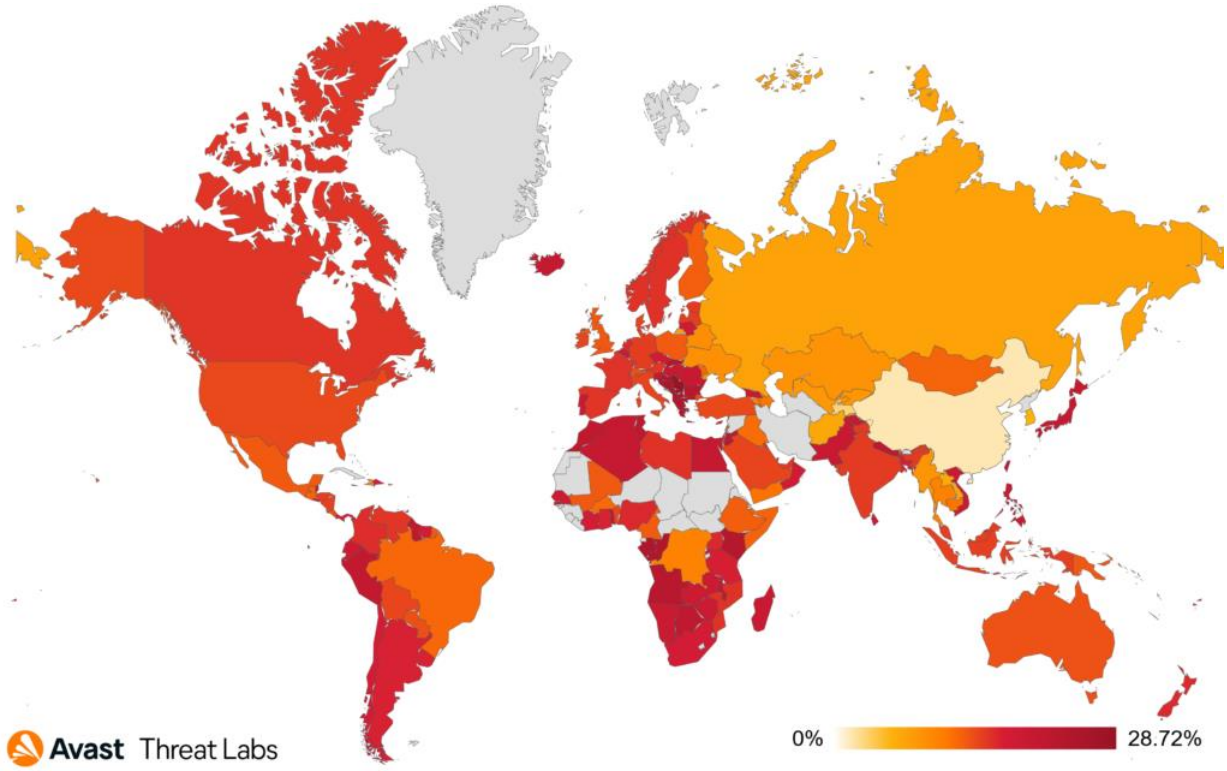
A scam is a type of threat that aims to trick users into giving an attacker their personal information or money. We track diverse types of scams which are listed below.

The significant increase in scam threats that we reported in Q2/2023 remained strong in the third quarter. As you can see in the following chart, we even saw a slight resumption of growth in mid-August.



Scam risk ratio over the last three quarters

In line with the trends observed in Q2, malvertising continues to serve as very strong tools for scammers, thanks to which they spread various categories of scams. This includes popular dating scams, or financial scams for example. These threats have maintained their strong position, but this is not the case with technical support scams. However, we are seeing the use of false reports of viruses being found to exploit them for sales purposes. Additionally, extortion email scams and phishing threats have both witnessed an uptick in popularity.



Global risk ratio for scam in Q3/2023

The countries most at risk of the scam attacks were Serbia, Kosovo, Montenegro, Albania, Croatia.

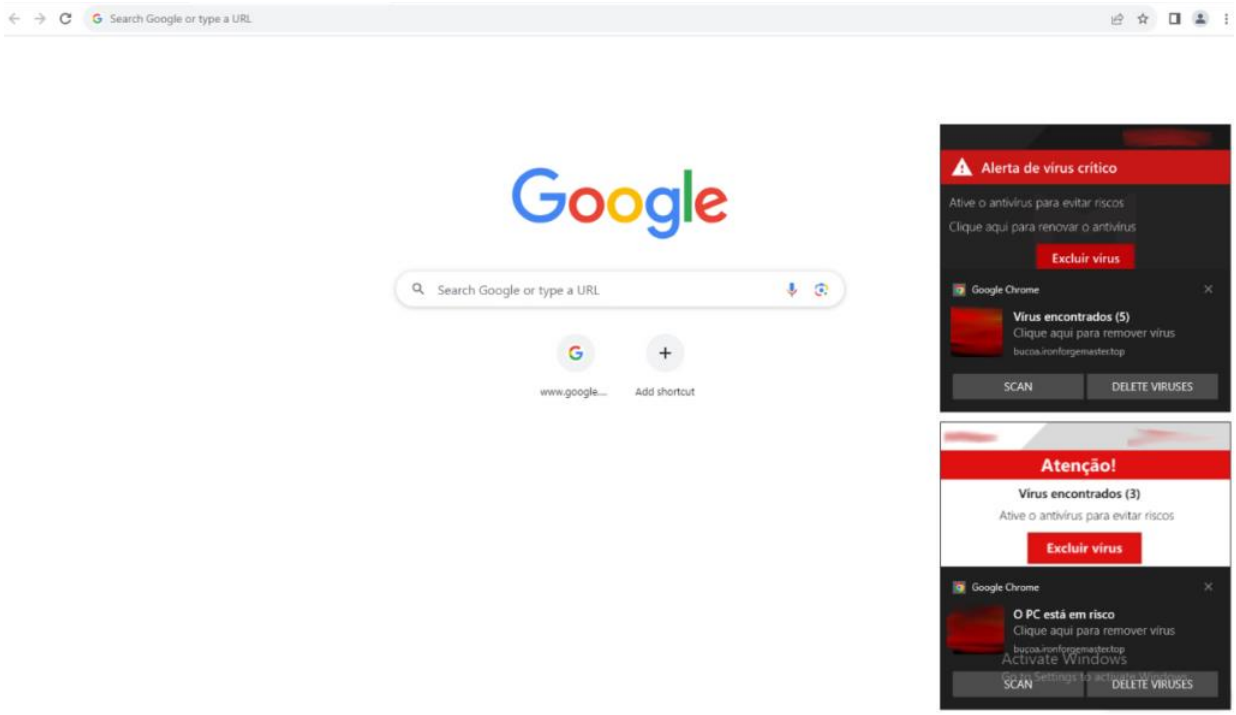
Countries where there was an increase in risk ratio are for example Japan +19%, Greece +17%, United States +14%, Austria +13%, or Germany +12%

Malvertising

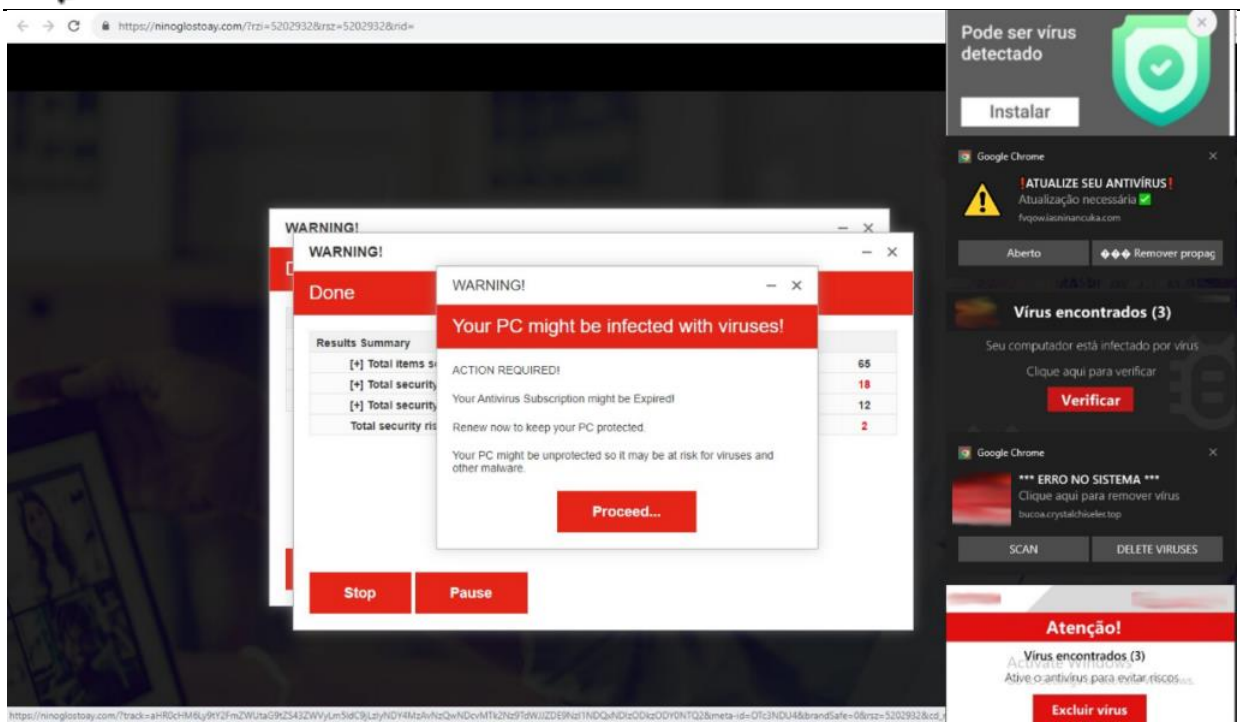
Malvertising is a malicious online advertising technique that involves the distribution of malware through online ads or, in some cases, in conjunction with browser push notifications. Cybercriminals use these seemingly legitimate ads to deliver malware to unsuspecting users' devices when they click on or interact with the compromised advertisements.

Cybercriminals are smart enough to make their malvertising pop-ups look genuine. Frequently, these fraudulent pop-ups exploit the recognizable antivirus company's logo. The goal is to convince users they are encountering a legitimate notification from an antivirus provider. These alerts typically display messages that a virus on a computer has been found and that the subscription plan has expired.

Upon clicking these deceptive pop-ups, unsuspecting users may find themselves redirected to a fake website. These fraudulent sites often take the form of straightforward phishing pages, where users are asked to enter personal credit card information under the guise of providing antivirus services. The scam can take many forms.



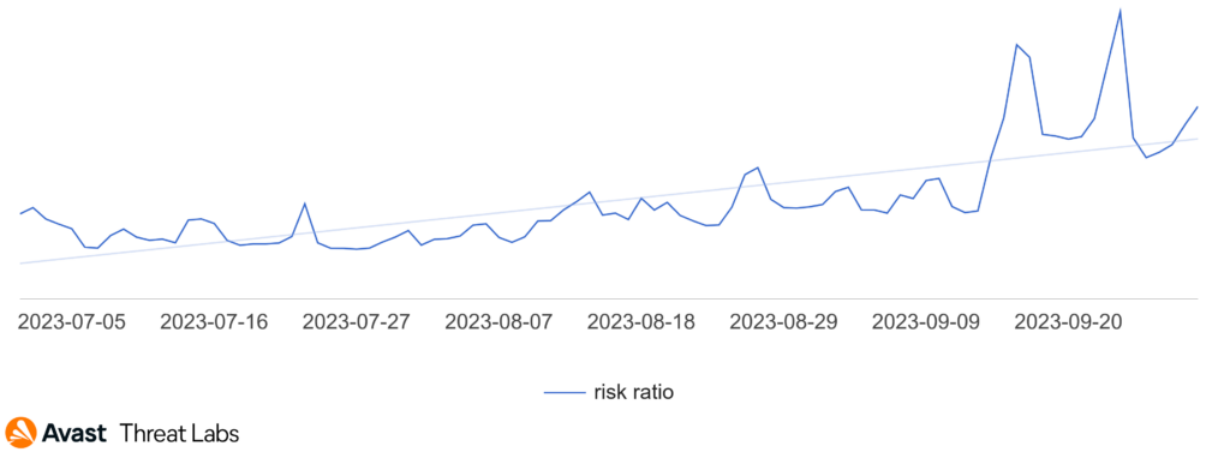
Verschiedene Popup-Fenster, die zum gleichen Betrug führen



Als Beispiel dient eine gefälschte Alarm-Landingpage mit Push-Benachrichtigungs-Popups

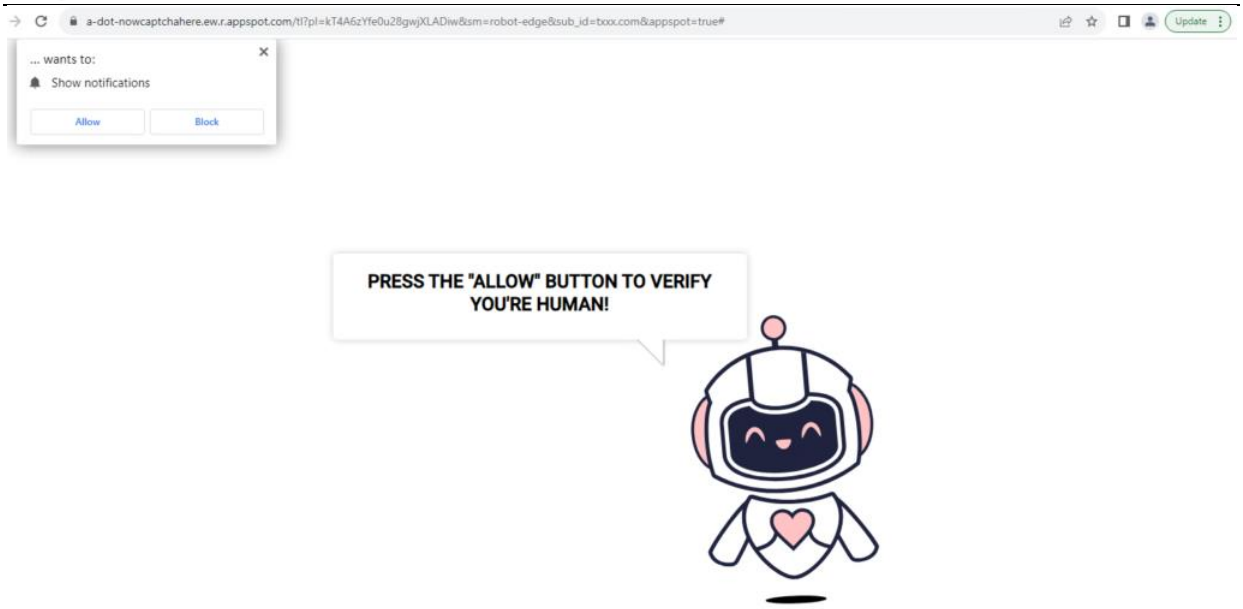
Wir haben bereits in früheren Berichten vor bösartigen Push-Benachrichtigungen gewarnt; Dieses Quartal ist keine Ausnahme. Diese Methode erfreut sich bei Betrügern nach wie vor großer Beliebtheit, da ihre Wirksamkeit insbesondere auf Mobiltelefonen immer noch beträchtlich ist.

As you can see in the below chart, the holiday season has ended not just for students but also for threat actors as there is a substantial surge in the volume of threat detections during September. The graph below represents detection of several types of malvertising. Within the month of September, we observed two prominent spikes in malvertising activity.



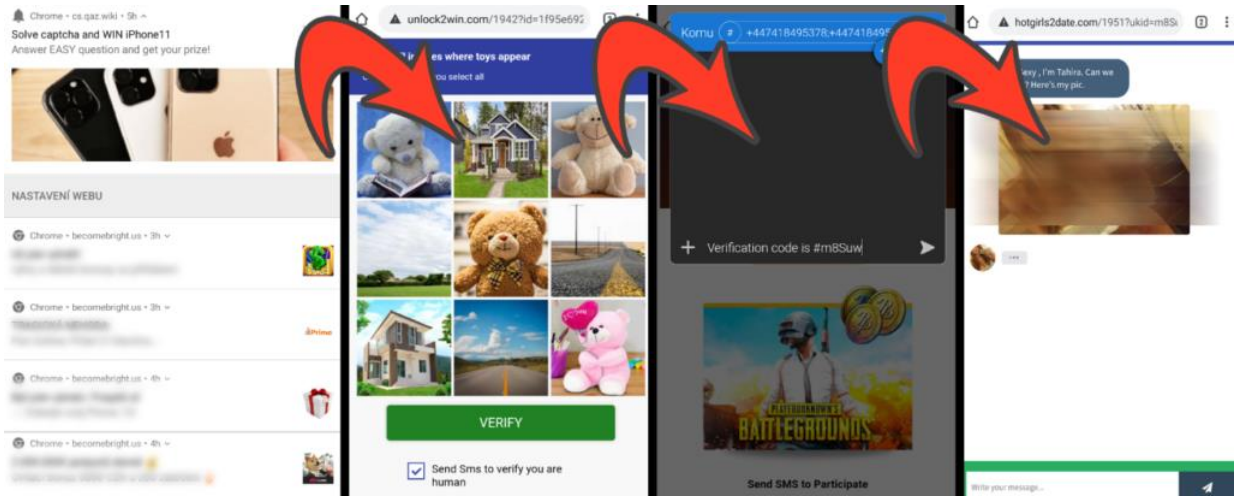
Graph illustrating a notable upswing in malvertising activity in Q3/2023

One of the most common examples of this malvertising was a page that fell into the push notification section that often appeared as part of a redirect chain. This page has multiple variations. The main purpose is to simply convince user to allow push notifications.



An instance of a website persuading users to grant permission for push notifications.

Push notifications can be especially effective on mobile devices, where they can also be disguised as system notifications, such as an unanswered call or a new text message.

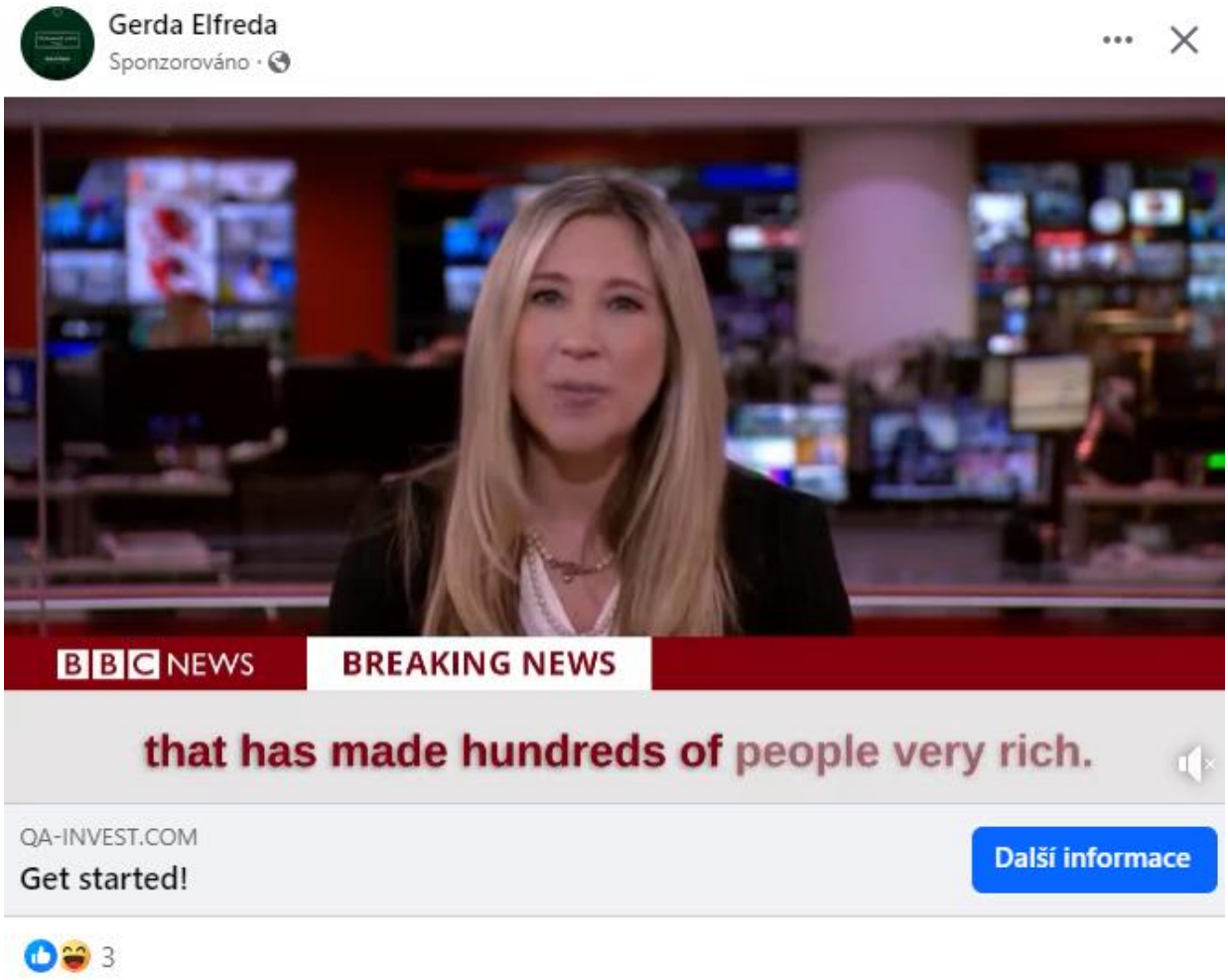


Example of a scam campaign using push notifications

Push notifications are not the only powerful tool for scammers. We have reported many times that scammers like to use advertising space on popular social networks. This way of promotion is especially dangerous because many users consider their social platforms to be a safe and personal space. Scammers also design their ads to attract attention, often by using catchy text or the faces of famous personalities. Thanks to this, the success rate of these campaigns is quite high.

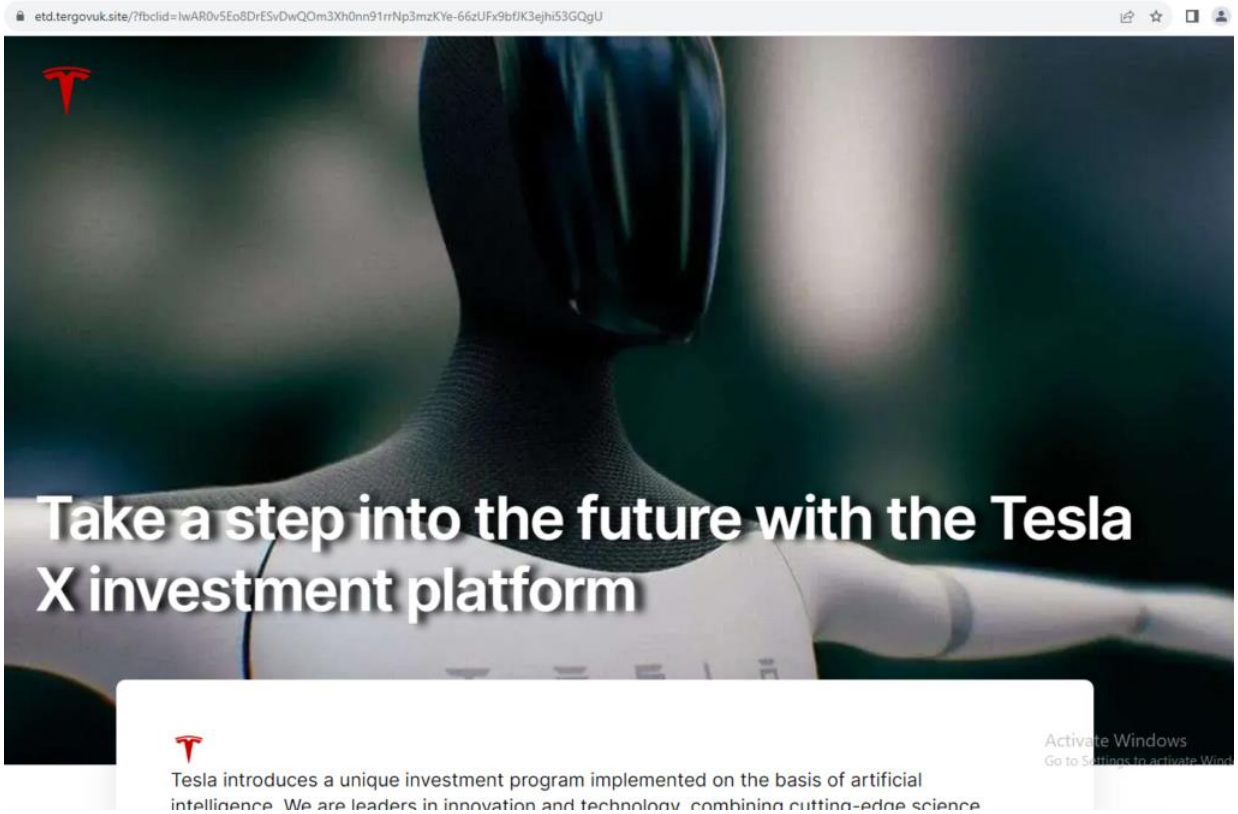
Another big advantage for scammers utilising social media ads is their ability to precisely target and tailor content to vulnerable users. Consequently, users may find their social media feeds full of these types of ads over time.

One adware example leading to a financial scam, which was seen in multiple languages.



Some scam ads are also found in video form

These above ad examples are from Facebook. In this case, these ads are part of a single fraudulent financial scam where scammers are trying to trick users into investing in an Elon Musk/Tesla project. After clicking on the ad, the user is redirected to a web page where they are informed about the great benefits and the certainty that this project is profitable.



Landing page supporting claims from social media advertising

The aim of the scammers in this example is to give the impression of professionalism. Part of the scam is also an appeal to the unrealistic possibility of buying through an ‘automatic robot’ that invests itself and ‘automatically’ earns money.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

SPECIAL BBC REPORT:

Tesla launches its newest platform Quantum AI™ - aims to help families become wealthier

Due to the financial crisis around the world, Tesla has launched a new project promising to help families become wealthier

2 days ago

Elon Musk's on the presentation Quantum AI™

By Shiona McCallum
Technology reporter

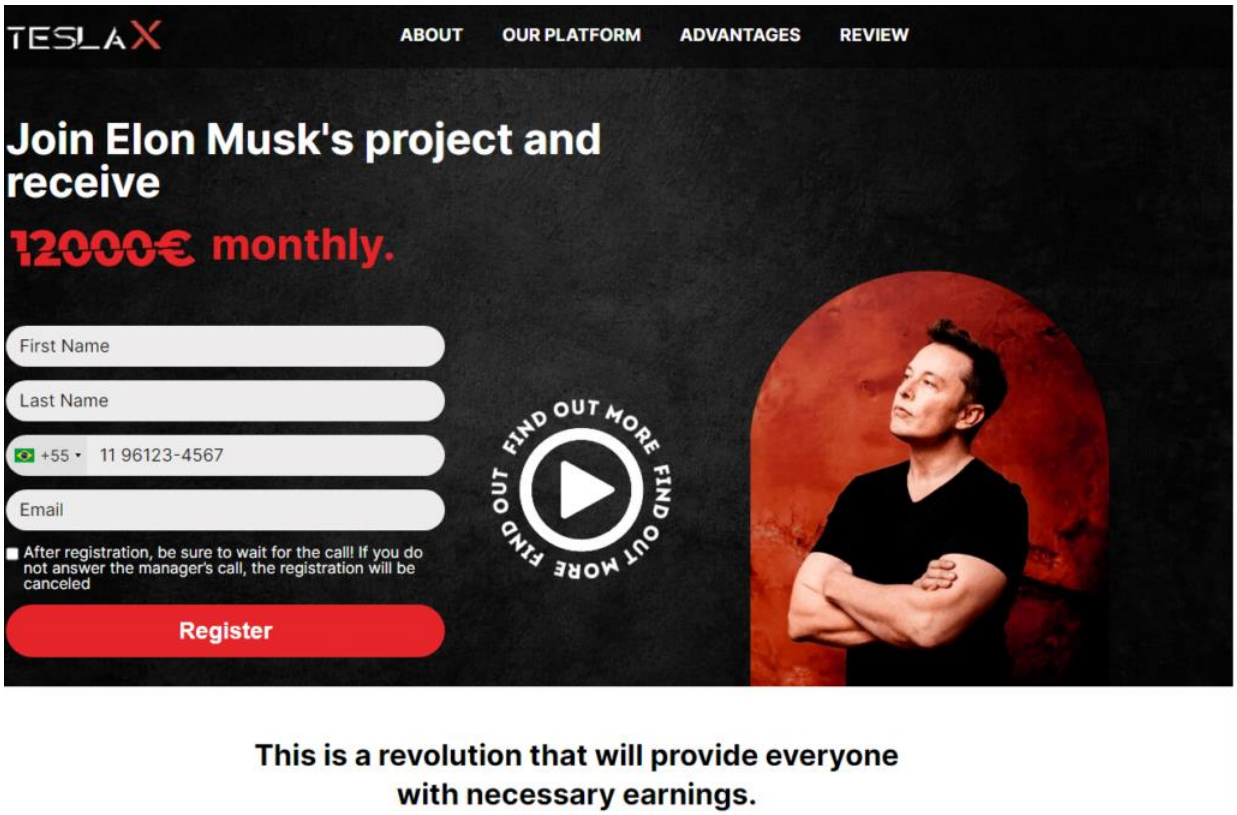
Key Facts

- It is well known that families around the world are suffering from financial crisis, businesses are shutting down and people are losing their jobs due to the recent global pandemic.
- Tesla corporation has decided to help those in need and started building its project **"Quantum AI™"**, investing €1.5 billion in bitcoin

Fake BBC News article ad

These fake sites can take many forms. Often there are variations that mimic the world's famous media such as BBC News and many others. These ads take advantage of the targeting of ads that social platforms allow them to do; the ads click through to websites that are created for users in individual countries that correspond to popular news sites in those countries.

The landing pages in this campaign also contain a registration form that requires users to enter their contact information. This information is then sent to the scammer, who then contacts the user either by email or, more often, by phone. Then the actual scamming effort is done over the phone.



Example registration form

After filling out these fraudulent forms, the user can expect a phone call from the fraudsters. The caller subjects the prospective buyer to a thorough questioning, giving the impression that the financial company is checking not only the solvency of the prospective buyer but also their professional and financial knowledge level. The prospective client is then persuaded to install a remote computer access application, in this case, usually AnyDesk.

To help avoid such scams, we strongly advise the following:

- do not disclose your personal information to people you do not know or cannot authenticate
- do not send photocopied personal documents
- do not send any printed credit card information
- do not give a code that would allow someone to access your computer remotely

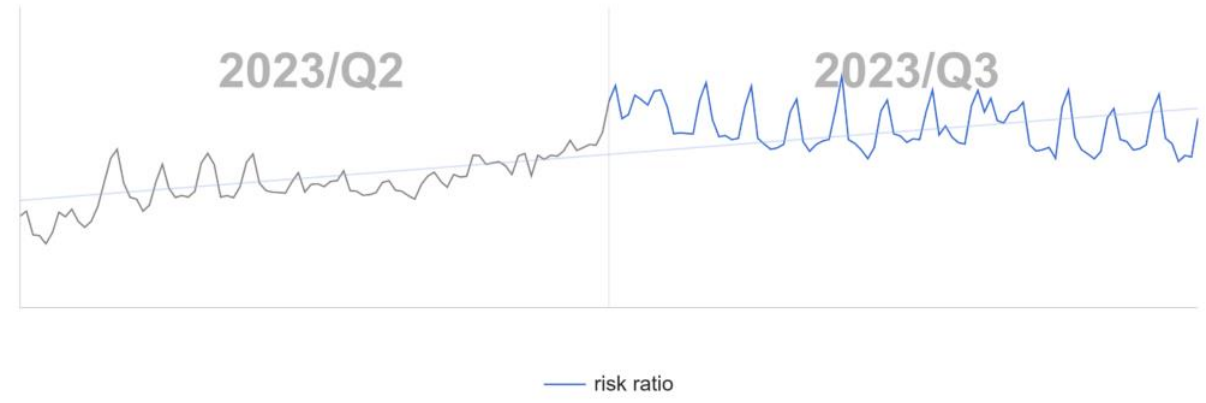
- if someone is remotely connected to your computer for any reason, do not log into your online banking
- do not forward or tell anyone SMS bank authorization codes
- do not authorize a payment to a stranger
- keep an antivirus program installed on your computer
- keep your online banking limits as low as possible and increase them only to the actual need to pay a specific payment

Dating Scams

Dating scams, also known as romance scams or online dating scams, involve fraudsters deceiving individuals into fake romantic relationships. Scammers adopt fake online identities to gain the victim's trust, with the goal of obtaining money or enough personal information to commit identity theft.

Dating scams have garnered increased attention from malicious actors due to the ever-growing popularity of online dating platforms. The accessibility and usual anonymity of these websites make them fertile ground for scammers seeking to exploit people's emotions and vulnerabilities. Bad actors create fake profiles and engage in emotional manipulation, gaining the trust of unsuspecting users before exploiting them financially or emotionally. As people turn to online dating in greater numbers, scammers see a larger pool of potential victims, which encourages them to invest more time and effort into these deceptive schemes.

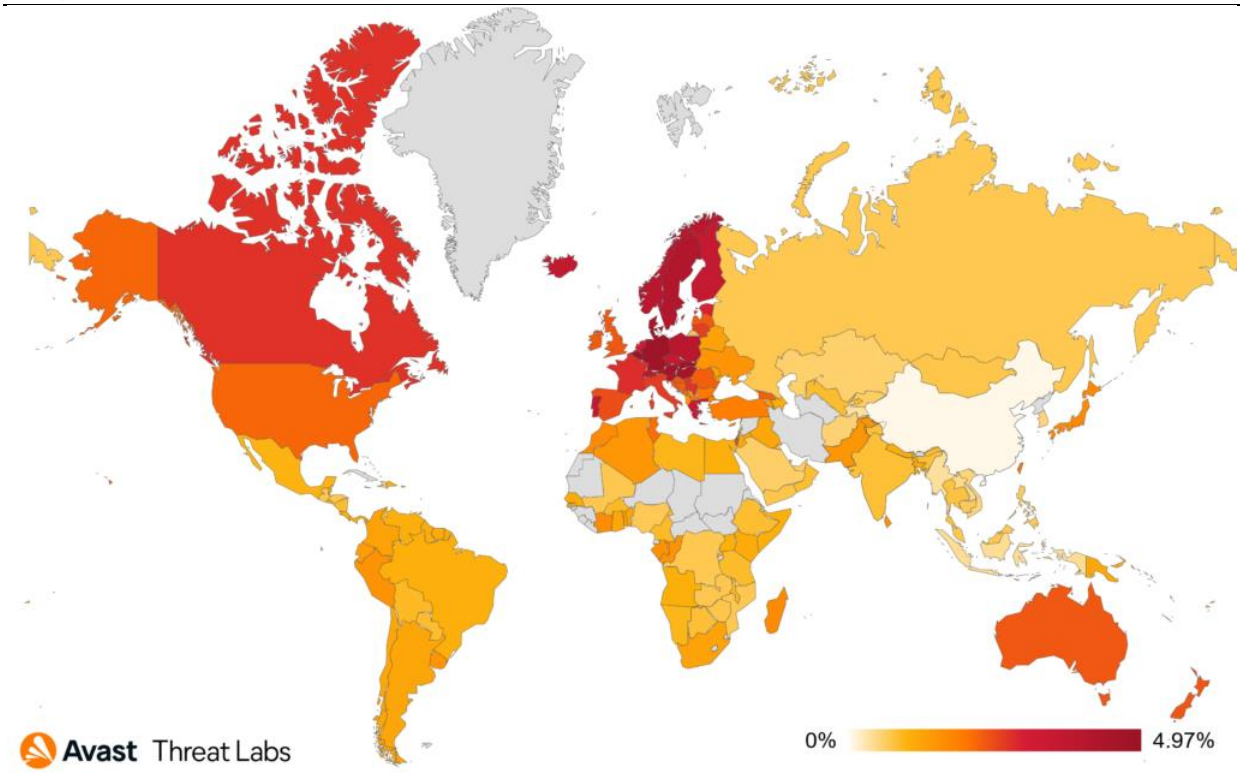
We observed a significant increase in dating scams during Q3/2023. The risk ratio of becoming a target rose by 34%.



Global risk ratio in Avast's user base regarding dating scams in Q3/2023

Dating scams are not confined to specific regions, but they do tend to be more prevalent in countries, such as those in Europe, the United States, Canada, and Australia. This can be attributed to a higher proportion of the population engaging in online dating due to increased internet accessibility and smartphone usage.

As illustrated by the heat map below, the highest risk ratio of getting involved in a dating scam is in Belgium (4.97%), Luxembourg (4.86%), Germany (4.76%), Slovakia (4.74%), and Austria (4.66%). In Canada, the risk ratio is 2.74%, closely followed by the United States with the risk ratio of 2.17%. For Australia, the risk ratio is 2.33%.



Map showing global risk ratio for dating scams in Q3/2023

Love-GPT

We have discovered a tool, which we call Love-GPT, that provides vast functionality over several different dating platforms, providing the capability to create fake accounts, interact with victims, bypass CAPTCHA, anonymize the access using proxies and browser anonymization tools, and more. The author is also experimenting with ChatGPT, the now-famous text-based generative AI, to provide them with more streamlined and believable texts. Because of that, we decided to name the tool Love-GPT. We have identified 13 different dating and social discovery platforms that the tool interacts with:

- Ashley Madison
- Badoo
- Bumble
- Craigslist
- DuyenSo
- Facebook Dating
- likeyou.vn
- MeetMe
- OkCupid
- Plenty of Fish (POF)
- Tagged
- Tinder
- Zoosk

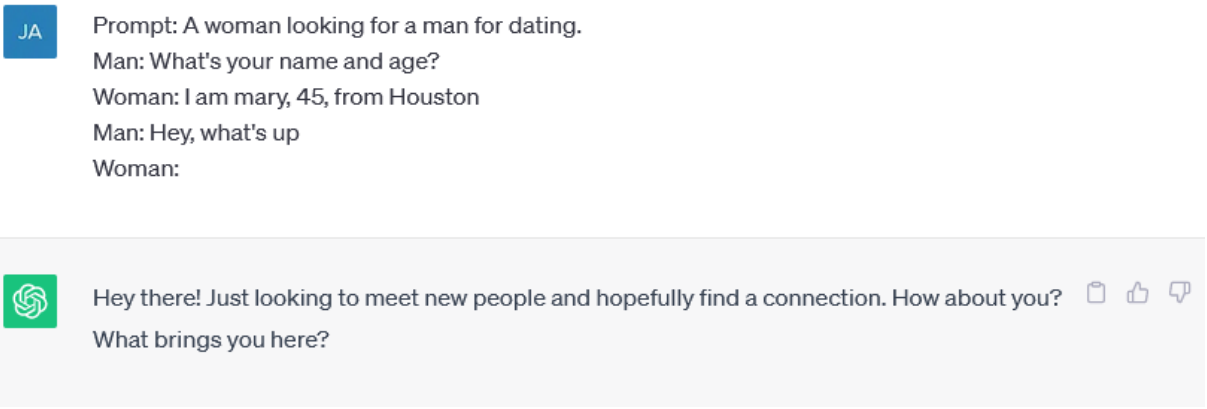
The tool uses ChatGPT API in attempts to streamline the texts. Overall, the tool contains these functionalities leveraging ChatGPT (both finished and under development):

- Create a fake profile description to be used on the dating platforms
- Read the inbox on the dating platform and reply to messages
- Ask for a phone number
- Write a first contact message
- Chat from a template

The tool uses “prompt” values in the API requests’ body to generate the output using ChatGPT. In some of the cases, the whole context is provided to guide ChatGPT for the more precise results:

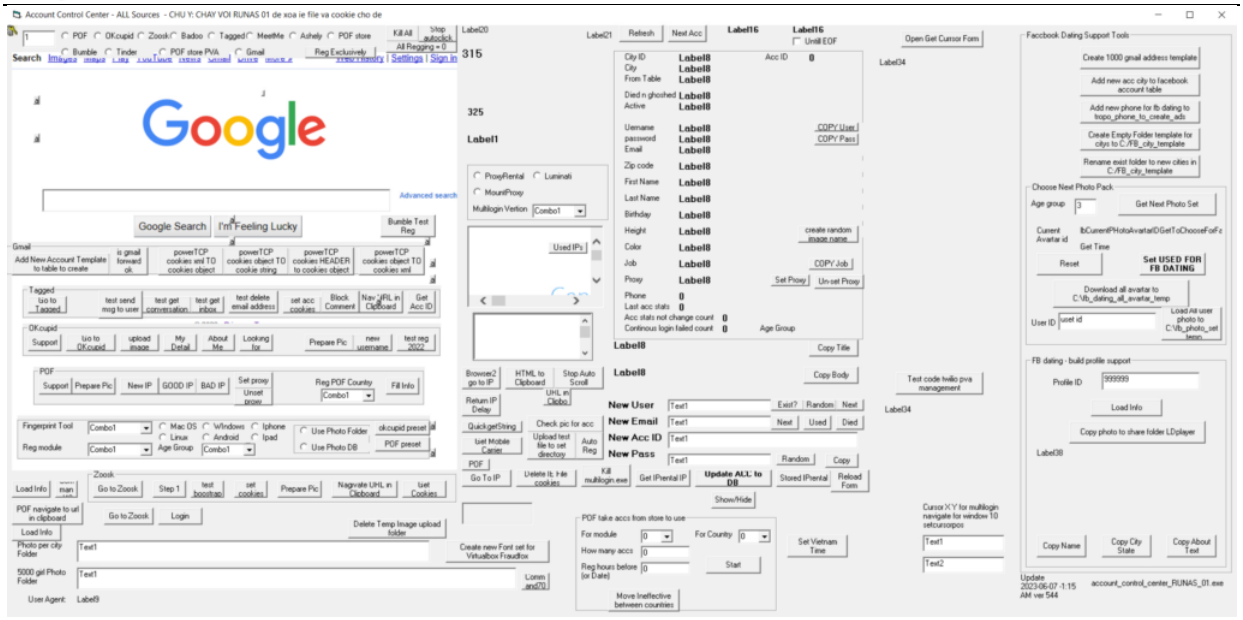
```
.text:004D9C50 aPromptAWomainL:                        ; DATA XREF: main_8EC130_GPT_openai_davinci_button+27D↓o
.text:004D9C50                                         ; main_8EC970_GPT_openai_turbo_button+27D↓o
.text:004D9C50                 text "UTF-16LE", '"prompt": "A womain looking for a man for dating.\n'
.text:004D9CB6                 text "UTF-16LE", 'Man: whats you name and age?\nWoman: I am mary, 45,'
.text:004D9D1C                 text "UTF-16LE", ' from Houston.\nMan: hey, whats up\nWoman:",',0
.text:004D9D76                 align 4
```

Just for the sake of demonstration, this is what ChatGPT usually returns for similar prompts:



This functionality provides an interesting insight into the upcoming trend of using highly believable texts leveraging generative AI and large language models (LLMs). We can already see that tools misusing the generative AI platforms are emerging and this is likely one of the first in-the-wild examples how the bad actors can misuse it.

Love-GPT is written in VB6 and contains many control panels for its operations. In total, the tool contains 58 different application forms. One of such form, essential for the whole toolset, can be found below and it is called Account Control Center.



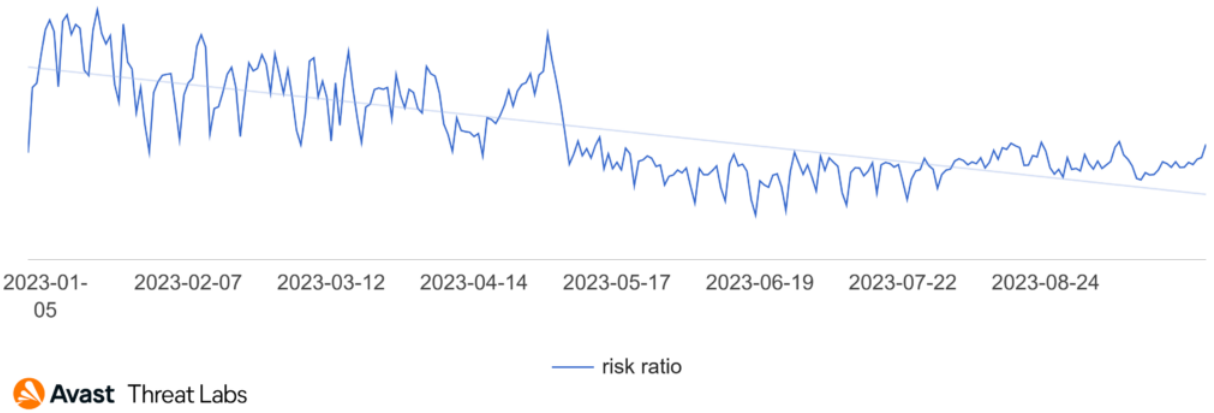
Account Control Center with a build-in browser

With this artillery, Love-GPT stays under the radar because no one can effectively distinguish connections coming from this specific tool and other regular users accessing the platforms. If you are interested in more technical details, check out our detailed analysis on Decoded.

Tech Support Scams

Tech support scam threats involve fraudsters posing as legitimate technical support representatives who attempt to gain remote access to victims' devices or obtain sensitive personal information, such as credit card or banking details. These scams rely on confidence tricks to gain victims' trust and often involve convincing them to pay for unnecessary services or purchase expensive gift cards. It is important for internet users to be vigilant and to verify the credentials of anyone claiming to offer technical support services.

The graph below demonstrates that there was no change for Q3. The downward trend from Q2 continued in the following quarter.

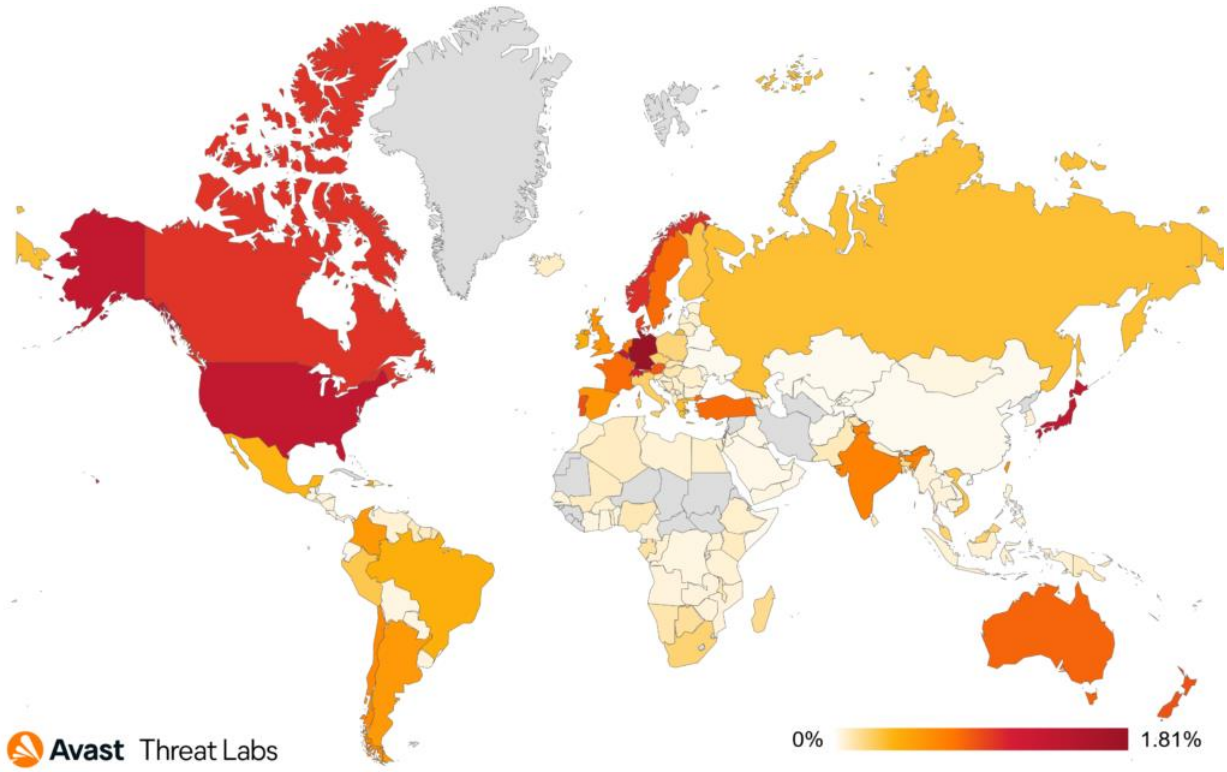


Graph illustrating a decline from the beginning of the year

Despite overall downward trend, a notable shift has been observed in the context of detection ratios among different countries. Compared to the previous quarter we have a change in terms of countries with the highest risk ratio. Japan came in second and was surpassed by Germany, Canada saw a big drop when it was surpassed by both the US and Switzerland.

Country	**Risk ratio**
Germany	1.81%
Japan	1.37%
United States	1.33%
Switzerland	1.19%
Canada	0.99%

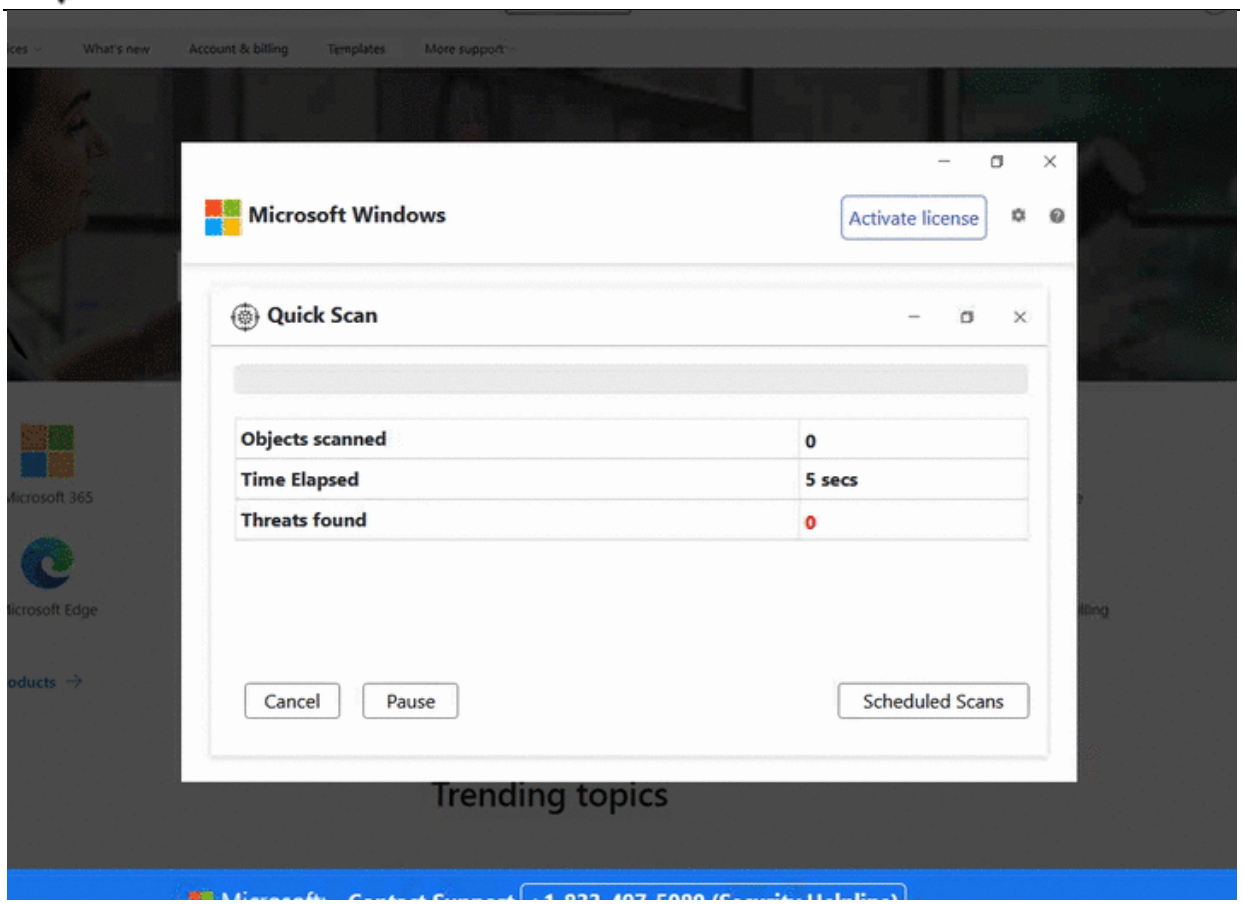
Even though we have seen a decline for this threat since the beginning of the year, the tech support scam still remains a global threat. Which is very effective, especially for inexperienced users.



Heatmap showing risk-ratio for Q3/2023

For all the years we have been monitoring tech support scams, the design of the site has barely changed. The main goal is to block the browser in such a way that the user is motivated to pick up the phone and call the provided phone number.

On following example, you can see the German variant. At the same time, Germany had the highest risk ratio in the third quarter despite the overall general decline.



The German variant of the most prevalent version of the TSS landing page

Das Aussehen der Seiten ist nicht das einzige eindeutig erkennbare Zeichen. Die URL-Zusammensetzung dieser Betrügereien ist nicht weniger interessant. Oft erkennt man die Art der Kampagne und deren Schwerpunkt. Manchmal enthalten sie sogar betrügerische Telefonnummern, wie in der folgenden Abbildung zu sehen ist.

```
https://main.d1r8o9e6vwez49.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=+1-844-681-0774
https://main.d1wva7figisbng.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=+1-877-544-5347
https://main.d21tl4murh9i3v.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=+1-844-672-0973
https://main.d26ecggelimxly.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=+1-844-339-6380
https://main.d21tl4murh9i3v.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=%09+1-844-672-0973
https://main.d31heemk415vae.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=+1-844-973-0992
https://main.d33ye1yt588h13.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=+1-877-958-3236
https://main.divwxzx8v5r3l.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=+1-844-652-0797
https://main.d9s79c00j0x7y.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=+1-844-652-0797
https://main.dcixxj7yyzfmp.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=+1-844-339-6380
https://main.di3j50b4tuxla.amplifyapp.com/8Sep_Ku_Win_Mac_Eng1_/werrx07/index.html?ph0ne=+1-844-339-6380
```

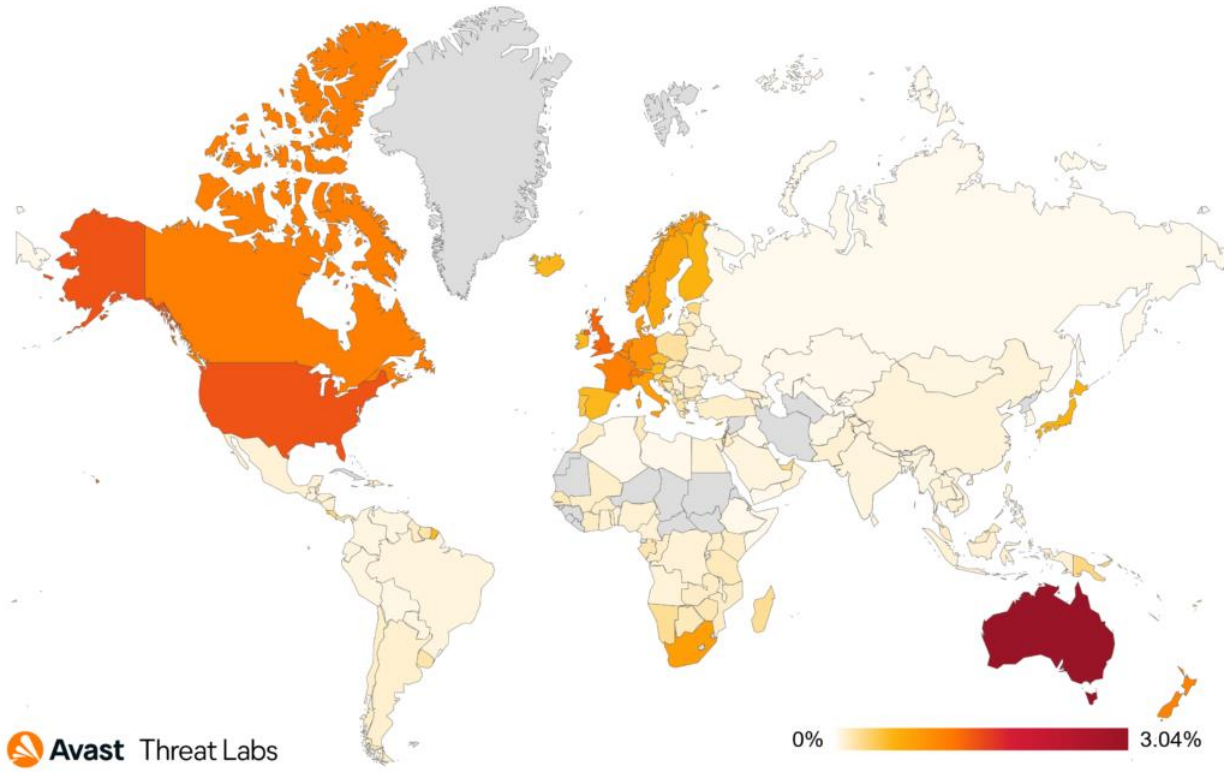
Ein Beispiel für URLs aus einer vorherrschenden Kampagne, die Telefonnummern von Betrügern enthalten

Rückerstattungs- und Rechnungsbetrug

Beim Rechnungsbetrug versenden Betrüger falsche Rechnungen oder Rechnungen für Waren oder Dienstleistungen, die nie bestellt oder erhalten wurden. Betrüger verlassen sich darauf, dass Rechnungen seriös aussehen, und verwenden häufig Firmenlogos oder andere Markenzeichen, um ahnungslose Opfer zu Zahlungen zu verleiten. Diese Betrügereien können besonders effektiv sein, wenn sie sich an Unternehmen richten, da die Mitarbeiter möglicherweise davon ausgehen, dass ein Kollege den Kauf getätigt hat, oder einfach die Rechnungsdetails übersehen. Es ist wichtig, alle Rechnungen und Abrechnungen sorgfältig zu

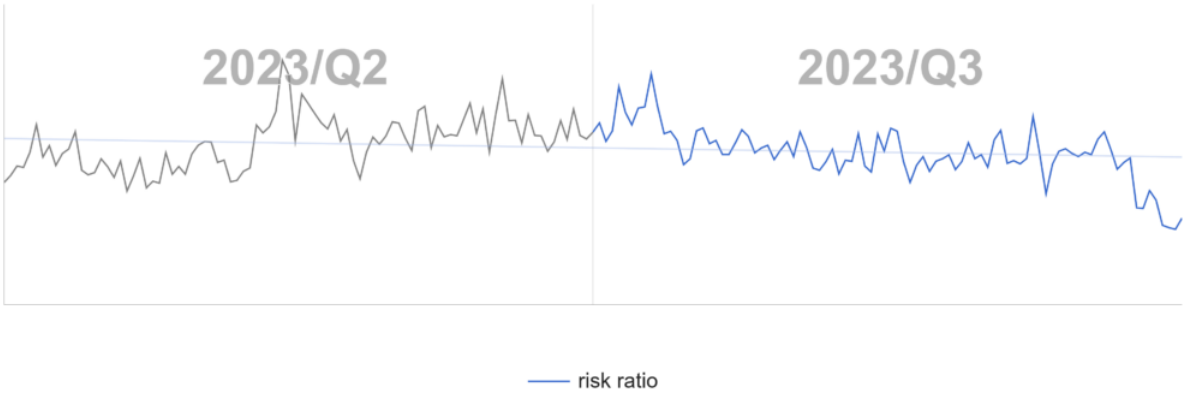
prüfen, bevor Zahlungen getätigt werden, und bei Betrugsverdacht die Legitimität des Absenders zu überprüfen.

In Australien war das vergangene Quartal eine Ausnahme von dem ansonsten konsistenten Trend, mit einem deutlichen Anstieg und einem plötzlichen Anstieg von E-Mail-Betrügereien. Bemerkenswert ist, dass der Anstieg der geschützten Kunden in Australien sogar den in den USA übertraf, die traditionell an der Spitze der Liste stehen. Die Anzahl der von uns beobachteten Bedrohungen in anderen Regionen blieb im Vergleich zu den Vorquartalen größtenteils auf einem sehr ähnlichen Niveau.



Refund and Invoice Scam risk ratio in Q3/2023

The highest uptick we observed was primarily due to the rise in Australia. Additionally, we noticed that smaller peaks usually occur at the beginning of the working week. This is when people generally sift through their mailboxes, and their vigilance may be lowered because of the larger volume of data they have to process. Therefore, one takeaway is that it definitely helps to take your time and sift through your emails in a peaceful manner, as rushing may increase the chance of falling victim to a scam.

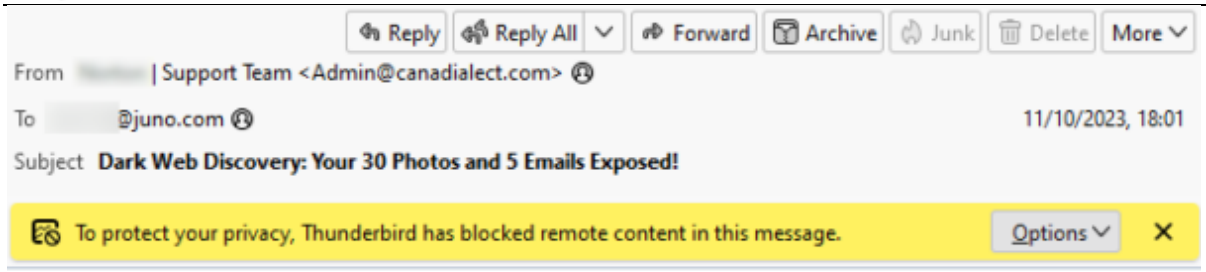


Avast Threat Labs

Refund and Invoice Scam in Q2/2023 and Q3/2023

In this quarterly report, we have chosen to spotlight a sample predominantly prevalent in Australia, as it experienced a nearly 30% increase compared to the previous period. This example was selected for its demonstration of many features increasingly noticeable in various other types of scams. The points we will mention should improve your ability to spot similar scams. Below is a breakdown of this deceitful email:

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55



Your subscription has expired

Wed,11 Oct-2023

Our Dark Web Monitoring has discovered 30 photos of you and 5 email addresses leaked in the Dark web

Dear ,

takes your online security seriously, and we have detected some alarming activity. Our Dark Web Monitoring service continuously scans the dark web and private forums, uncovering unsettling findings:

- **30 Photos of You:** we've found 30 photos of you circulating on the dark web.
- **2 Email Addresses:** we've identified 2 email addresses associated with you.

subscription is highly recommended to protect your device. We've activated a special discount for you to use on Wed,11 Oct-2023.

LIMITED TIME OFFER:

(80%) renewal discount Today

Name	
Email	@juno.com
Discount:	(80%) renewal discount Today
LIMITED TIME OFFER:	Wed,11 Oct-2023

Renew Now!

Example of a Refund and Invoice Scam seen in Q3/2023

This scam email contains a few typical scam traits:

- **Attention-Grabbing Subject Line**: "Dark Web Discovery: Your 30 Photos and 5 Emails Exposed!" By creating a sense of immediate danger, the sender aims to provoke curiosity and urgency.
- **Impersonation of a Legitimate Entity**: The email is supposedly from a "Support Team", which sounds official and trustworthy. However, the domain '@canadialect.com' raises eyebrows. Always double-check the authenticity of the domain.
- **Urgency and Fear**: The email highlights that the recipient's "subscription has expired," implying prior engagement or services with them. It also claims a discovery of personal photos and email addresses on the Dark Web.
- **Detailed Alarming Findings**: The message dives deeper into the 'findings', mentioning "30 photos of you" and "2 email addresses" associated with the recipient found in dark web forums. Providing specifics makes the scam seem more credible.
- **A Tempting Offer**: Following the alarming statements, there is a solution offered – a "(80%) renewal discount Today" on their service. This discount plays on the human tendency to seek quick resolutions when faced with threats.
- **Clear Call to Action**: The bold "Renew Now!" button at the end of the email serves as a clear directive for the panicked reader. Clicking on such links often leads to phishing sites or direct financial scams.

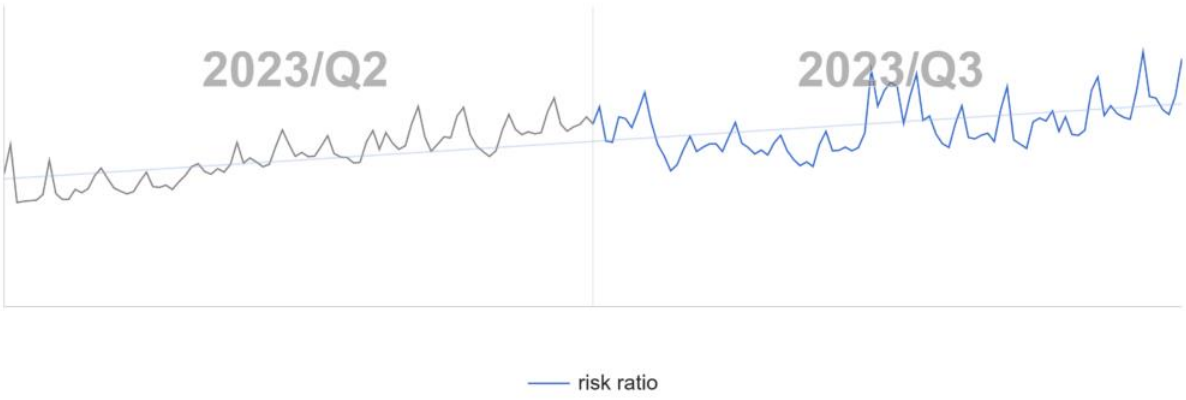
As a parting word of advice, always be skeptical of unsolicited emails, especially those that invoke fear and urgency. Verify claims independently and avoid clicking on links or downloading attachments from unknown senders.

Phishing

Phishing is a type of online scam where fraudsters attempt to obtain sensitive information including passwords or credit card details by posing as a trustworthy entity in an electronic communication, such as an email, text message, or instant message. The fraudulent message usually contains a link to a fake website that looks like the real one, where the victim is asked to enter their sensitive information.

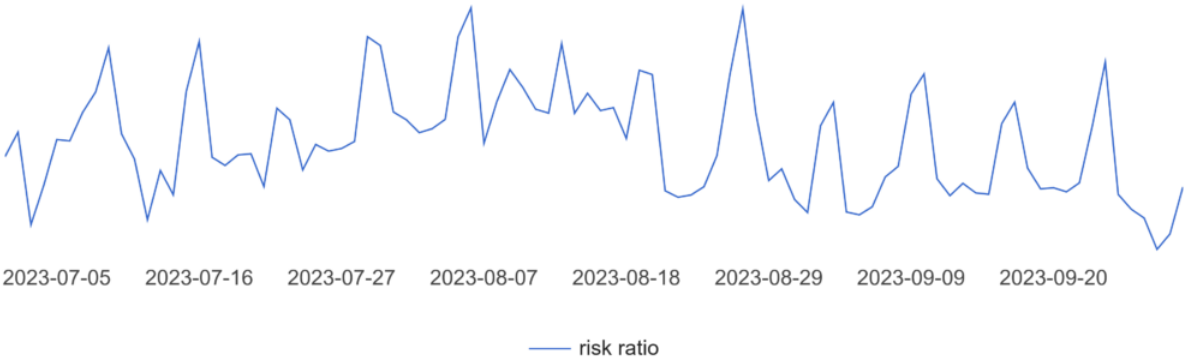
In the Q2/2023 Threat Report, we pointed out that phishing activity was picking up. Now we can confidently confirm that our estimates were correct and after a dip in mid-July, a wave of new samples arrived in August, which then represents a big jump on the chart.

The following graph illustrates the activity of phishing threats across two quarters.



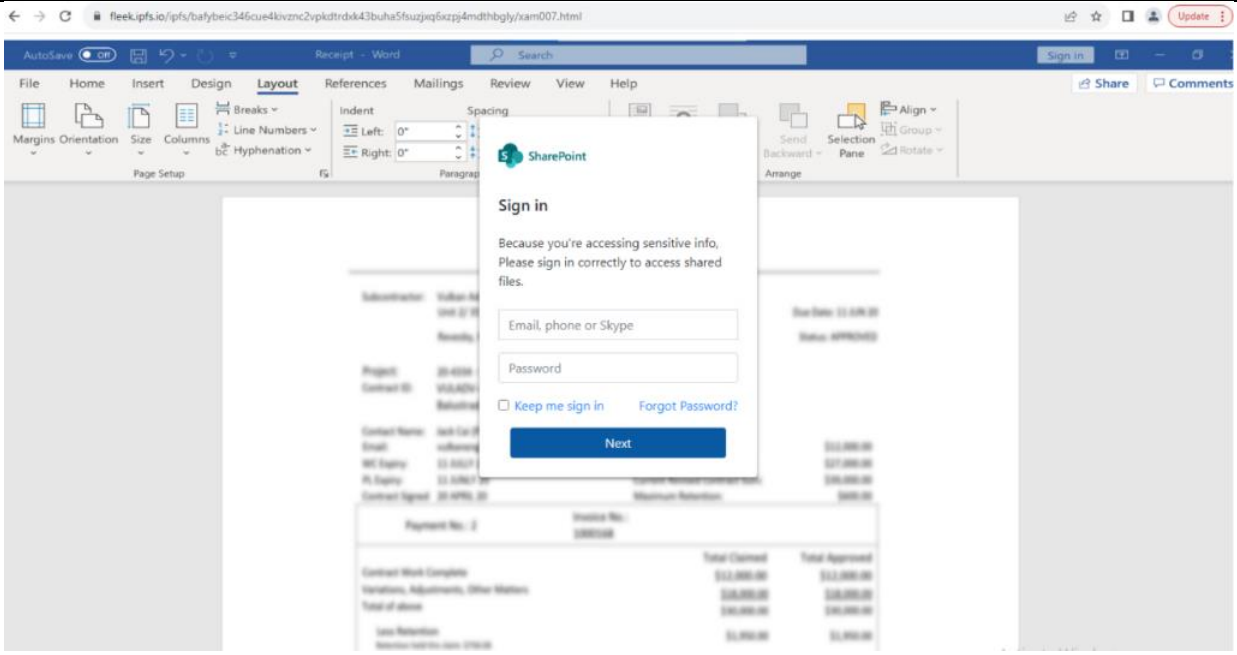
Risk ratio for Q2-Q3/2023 of phishing threats

Furthermore, we have observed an emerging trend in phishing delivery methods. Over the past few months, there has been a notable uptick in the use of InterPlanetary File System (IPFS) to disseminate phishing content. This decentralized protocol, designed for storing and sharing files, has become an attractive avenue for cybercriminals.



IPFS-based attacks and the related risk ratio in Q3/2023

In addition to IPFS, we have also witnessed cybercriminals turning to the CAR file format, which poses a unique challenge for traditional HTML scanners, allowing it to potentially bypass detection. This exclusive preference for such hosting methods among hackers can be attributed to their ease of deployment and the added complexity in takedown procedures, providing an advantageous environment for malicious activities.



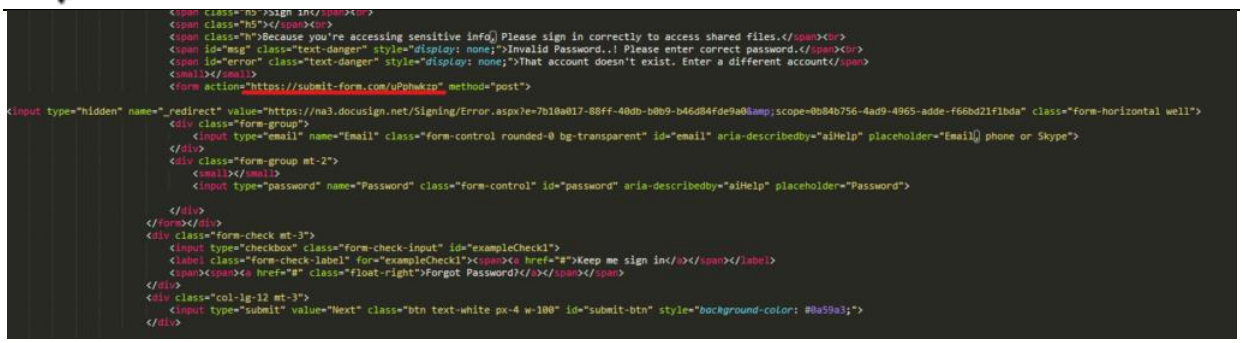
Example of a phishing page using IPFS

Campaigns that are running on IPFS infrastructure quite often use some type of obfuscation. In most cases these are very basic types and their deobfuscation is very simple.

In this prevalent example you can see that the HTML code itself has been encoded to make it unreadable. Therefore, the JavaScript feature unescape() is used. Despite the fact that the use of this function is not recommended, because it has been deprecated, it often appears in IPFS samples.

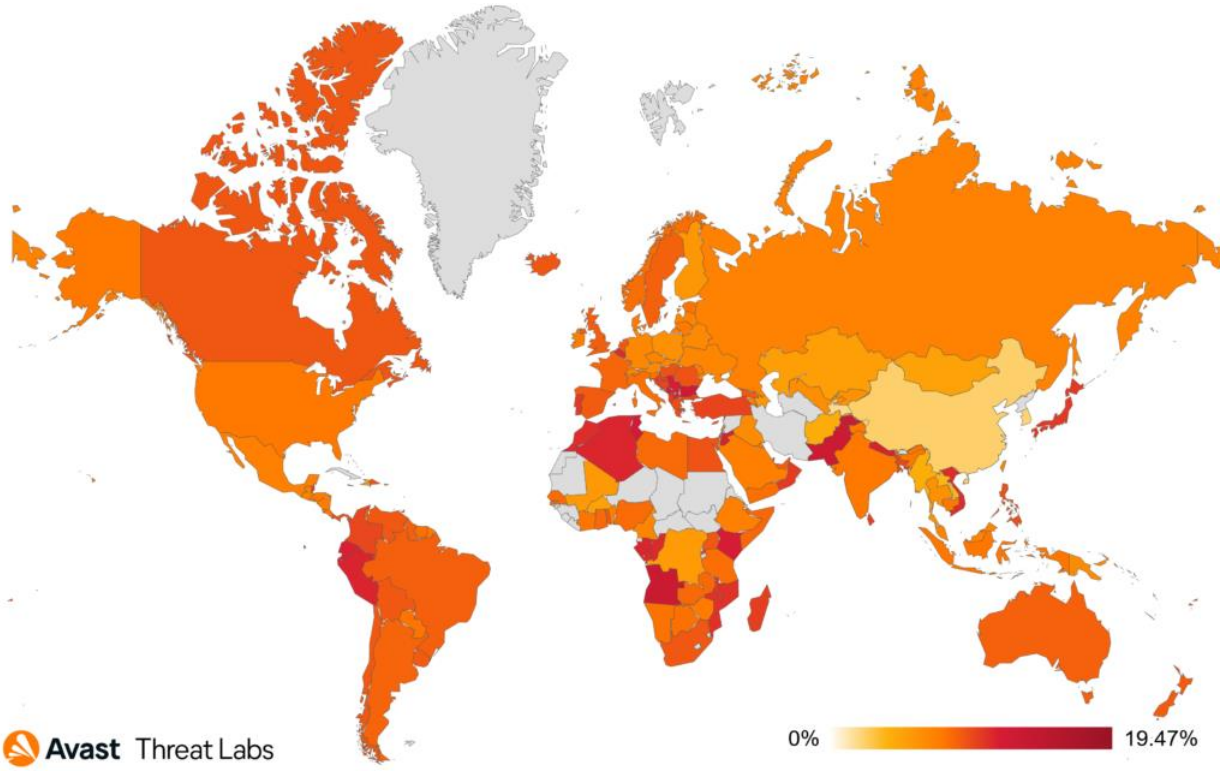
Source code is typically obfuscated

In decoded HTML source code, you can see that scammers are using submit-form.com endpoint for credentials submission.



Deobfuscated source code of IPFS phishing sample

Analyzing the data for Q3/2023 Argentina, Brazil, Mexico, and Spain are countries with a significant increase in Q/Q risk ratio for phishing. Countries with the highest overall risk ration are Macao with 19.47%, Angola with 13.14% or Pakistan with risk ratio of 12.8%.



Global risk ratio of phishing in Q3/2023

Phishing has long been the classic and primary way to steal valuable data from users. A growing trend points out that although this is a relatively old method, it is far from being obsolete.

Alexej Savčin, Malware Analyst
Martin Chlumecký, Malware Researcher
Branislav Kramár, Malware Analyst
Bohumír Fajt, Malware Analysis Team Lead
Jan Rubín, Malware Researcher

Mobile-Related Threats

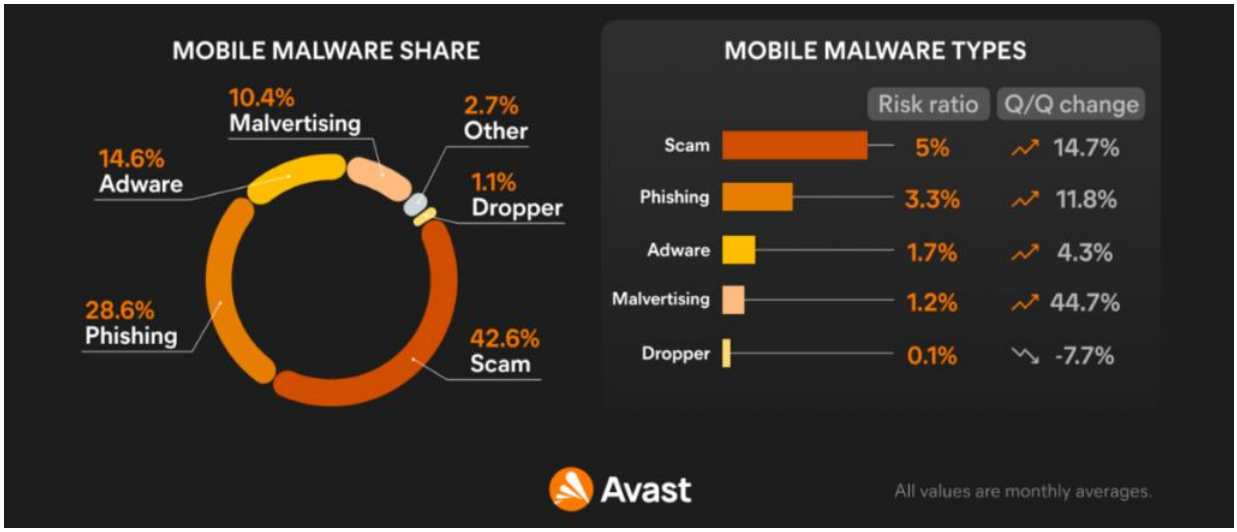
Ein weiteres Quartal, eine weitere Reihe abwechslungsreicher und interessanter Entwicklungen in der mobilen Bedrohungslandschaft. Im Zusammenhang mit der eskalierenden Situation zwischen Israel und Palästina imitiert eine Spyware eine in Israel eingesetzte Raketenwarnanwendung mit der Absicht, Opferdaten zu stehlen. Bemerkenswert ist auch der Xenomorph-Banker, der neue Funktionen hinzugefügt hat und sich zusammen mit einem Windows-Info-Stealer verbreitet.

Eine neue Art von unsichtbarer Adware zeigt Werbung an und klickt darauf, während der Bildschirm des Geräts ausgeschaltet ist, was zu betrügerischen Werbeeinnahmen führt und den Akku und das Datenvolumen des Opfers erschöpft. Wir haben in diesem Quartal auch mehrere neue Versionen von SpyNote beobachtet, von denen eine die Grenze zwischen Spyware und Banker-Malware überschreitet.

Beliebte Mods für Messenger-Anwendungen wie Telegram, Signal und WhatsApp werden weiterhin für die Verbreitung von Spyware missbraucht. Und schließlich verbreiten sich SpyLoans weiterhin im PlayStore und bedrohen gefährdete Opfer mit Erpressung.

Daten zu Web-Bedrohungen in der mobilen Landschaft

Wie beim Desktop haben wir in diesem Quartal auch Daten zu Web-Bedrohungen in unseren mobilen Bedrohungsbericht aufgenommen. Diese zusätzlichen Daten spiegeln eine Neuordnung der häufigsten Bedrohungen wider, denen mobile Benutzer heute ausgesetzt sind. Wie die Grafik unten zeigt, sind Betrug, Phishing und Malvertising für die Mehrzahl der blockierten Angriffe auf Mobilgeräten verantwortlich.



Grafiken, die die häufigsten Bedrohungen im mobilen Bereich im dritten Quartal 2023 zeigen

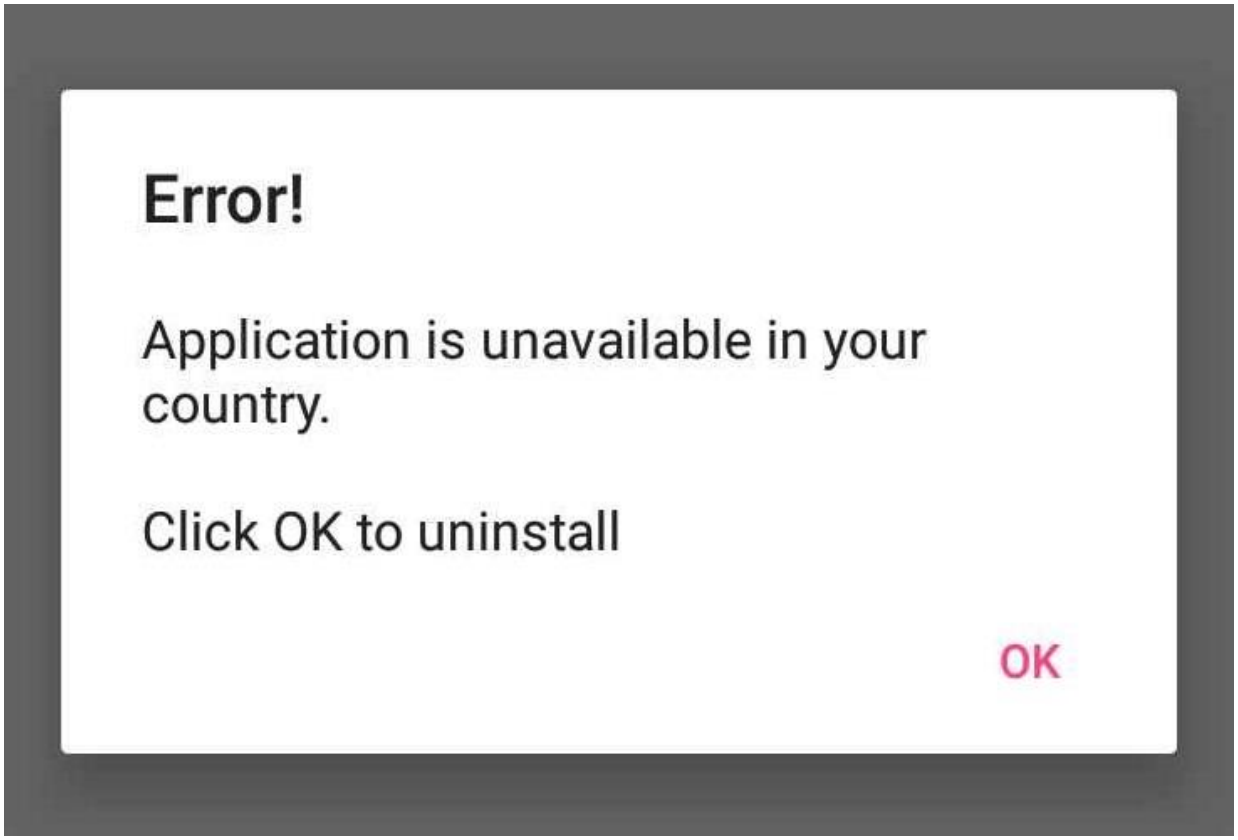
Es macht Sinn, dass webbasierte Bedrohungen den Großteil der blockierten Angriffe sowohl auf Mobilgeräten als auch auf Desktops ausmachen. Bei jeder bösartigen App auf Android ist eine Benutzeraktion erforderlich, um sie zu installieren. In den meisten Fällen erfordert die Malware, dass der Benutzer einige Berechtigungen aktiviert, damit die bösartige Funktionalität aktiviert werden kann. Im Gegensatz dazu können webbasierte Betrügereien, Phishing und Malvertising durch normale Surfaktivitäten auftreten, die die meisten mobilen Benutzer täglich durchführen. Diese Webbedrohungen können auch in privaten Nachrichten, E-Mails, SMS und anderen enthalten sein.

Adware Becomes Nearly Invisible

Adware threats on mobile phones refer to applications that display intrusive out-of-context adverts to users with the intent of gathering fraudulent advertising revenue. This malicious functionality is often delayed until sometime after installation and coupled with stealthy features such as hiding the adware app icon to prevent removal. Adware mimics popular apps such as games, camera filters, and wallpaper apps, to name a few.

Despite the addition of web threats data, adware remains one of the most prevalent threats on mobile and retains its top spot among traditional malware apps. Serving intrusive advertisements to its victims with the intent of gathering fraudulent ad revenue, these apps pose a danger and annoyance to both users and advertisers alike.

At the top of the adware list is HiddenAds, followed by MobiDash and FakeAdBlock strains. While both MobiDash and FakeAdBlock have seen over 40% decrease in protected users, HiddenAds is on the rise again with a bump of 15% in protected users. All three strains share some features such as hiding their icon and displaying out-of-context full screen ads that annoy victims. HiddenAds has historically relied on the PlayStore as a mode of spread, while the others generally rely on 3rd party app stores, malicious redirects, and advertisements. Of note is a recent addition to the stealth features of these adware apps; once installed, they display a fake error stating the app is not available in the victim's region or country with an 'installation failed' message. Coupled with hiding its icon, the adware conducts its malicious behavior in the background while the victim remains unaware of the source of the fraudulent ads.

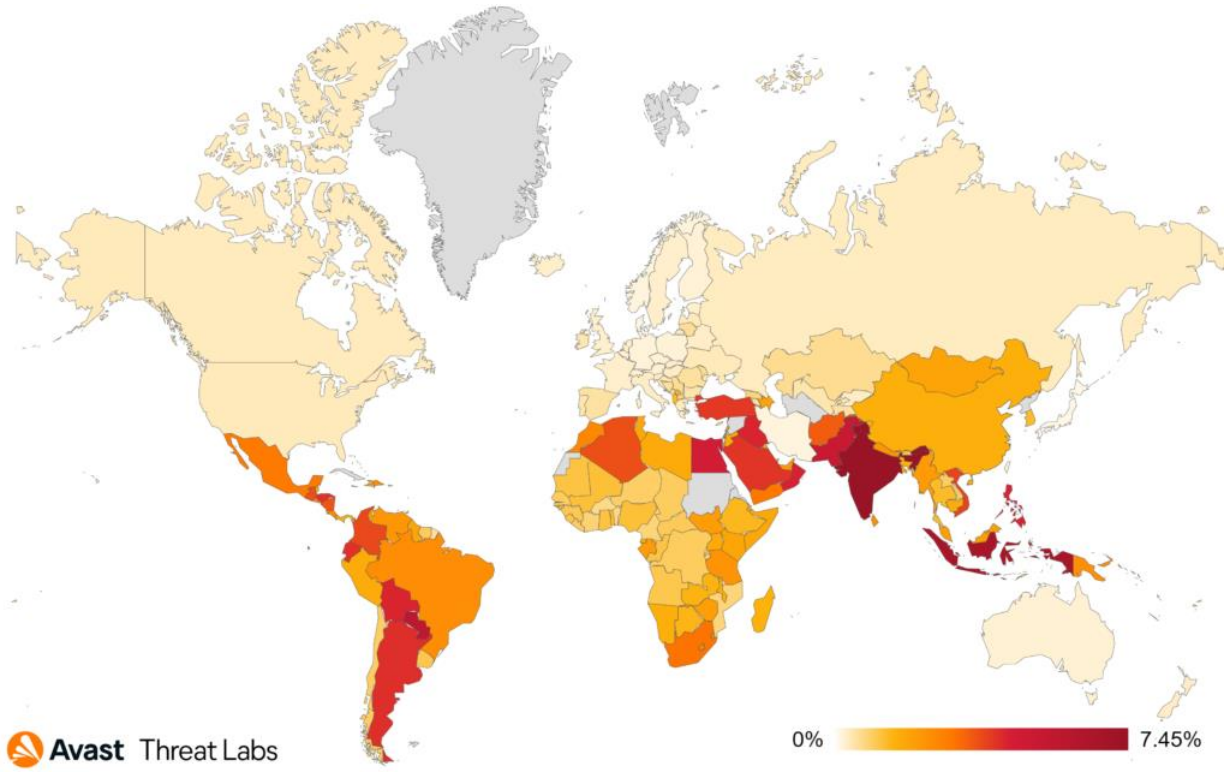


MobiDash adware tries to trick its victim by displaying a fake error message after install

This quarter a new batch of adware dubbed Invisible Adware has snuck onto the PlayStore and gathered over two million downloads. True to their name, these applications try and display advertisements while the device screen is off. In essence, the victim would be unaware their phone is displaying ads while the malicious actors gather revenue through fake clicks and ad views. However, this will likely impact the device battery and potentially incur data charges, while at the same time contributing to ad fraud. The applications request permissions to run in background and ignore battery optimization to conduct their activity. While observed behavior is that of ad fraud, there is also potential for installing other malware or visiting malicious websites.

The average daily protected users slightly increased when compared to last quarter. MobiDash and FakeAdBlock strains have gone down while HiddenAds continue to increase in popularity. Another campaign on PlayStore contributes to the steady numbers this quarter.

Brazil, India, and Argentina are again at the top of the most affected users by adware this quarter. Argentina saw a 14% increase in monthly affected users. India, Indonesia, and Paraguay have the highest risk ratio this quarter, meaning users is these countries are most likely to encounter adware.



Global risk ratio for mobile adware in Q3/2023

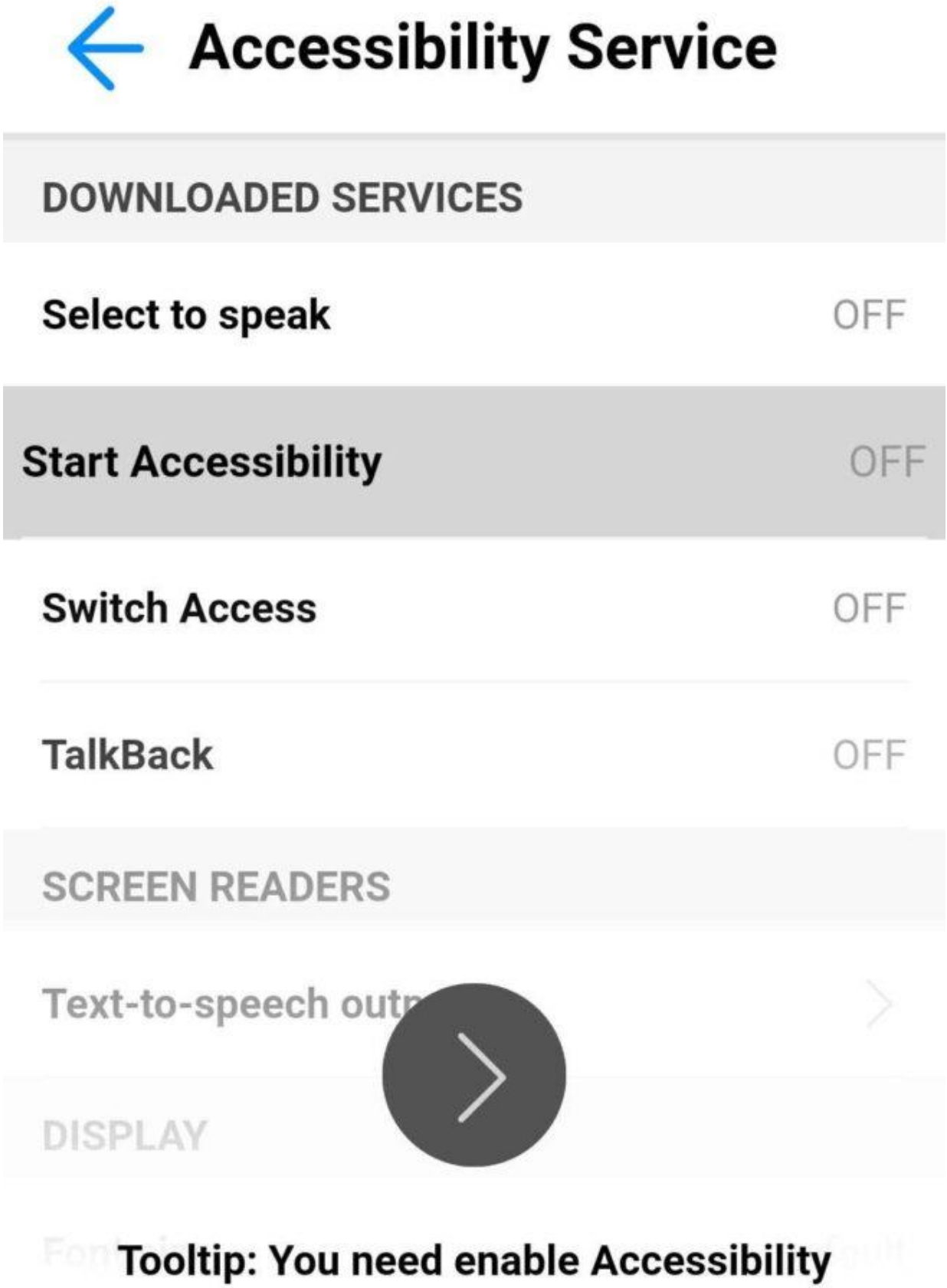
Bankers Welcome SpyNote into the Fold

Bankers are a sophisticated type of mobile malware that targets banking details, cryptocurrency wallets, and instant payments with the intent of extracting money. Generally distributed through phishing messages or fake websites, Bankers can take over a victim's device by abusing the accessibility service. Once installed and enabled, they often monitor 2FA SMS messages and may display fake bank overlays to steal login information.

Banker evolution continues this quarter with several new strains alongside updates to existing ones. Xenomorph makes a return with some new features, GoldDigger makes an entrance and SpyNote breaches the divide between spyware and bankers. Despite the new arrivals and updates, bankers overall have been on a steady decline in terms of protected users in our telemetry for the last few quarters. Cerberus/Alien maintains its top spot this quarter, trailed by Coper and Hydra strains. We observe an over 20% decrease in monthly average protected users this quarter on all top three banker strains.

Xenomorph is back after a few months hiatus and has evolved again with several added features and a new method of spread. It appears that this new campaign mainly targets bank users in Spain, US and Portugal as well as adding crypto wallets to its repertoire. Using tailored phishing websites disguised as chrome updates, Xenomorph tricks victims into downloading its malicious APK. Once installed, it uses the accessibility service to take over the device, monitoring 2FA messages and can display hundreds of fake bank overlays to its victim to steal login credentials. New features include keeping the device awake, a mimic mode that disguises the malware further and hides its icon, and lastly it can click anywhere on the device's screen. Interestingly, Xenomorph was observed to be served alongside RisePro, a Windows based info stealer that also targets banking details and crypto wallets. This may point to a coordinated effort between various actors or a single actor behind multiple strains of malware.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55



A 'tooltip' displayed to the victims of Xenomorph once it is installed on the device

A banker targeting victims in Vietnam pretending to be a government portal or a local energy company has been discovered and codenamed GoldDigger. It uses Virbox Protector, a publicly available software that can obfuscate code and prevent both dynamic and static analysis. This appears to be a growing trend in Southeast Asia in recent years, as the use of advanced obfuscation can mean the malware goes undetected for longer. GoldDigger uses fake websites that imitate the PlayStore or phishing in private messages to spread itself. Once on the device, it can steal 2FA SMS as well as personal information and banking credentials.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Chính phủ

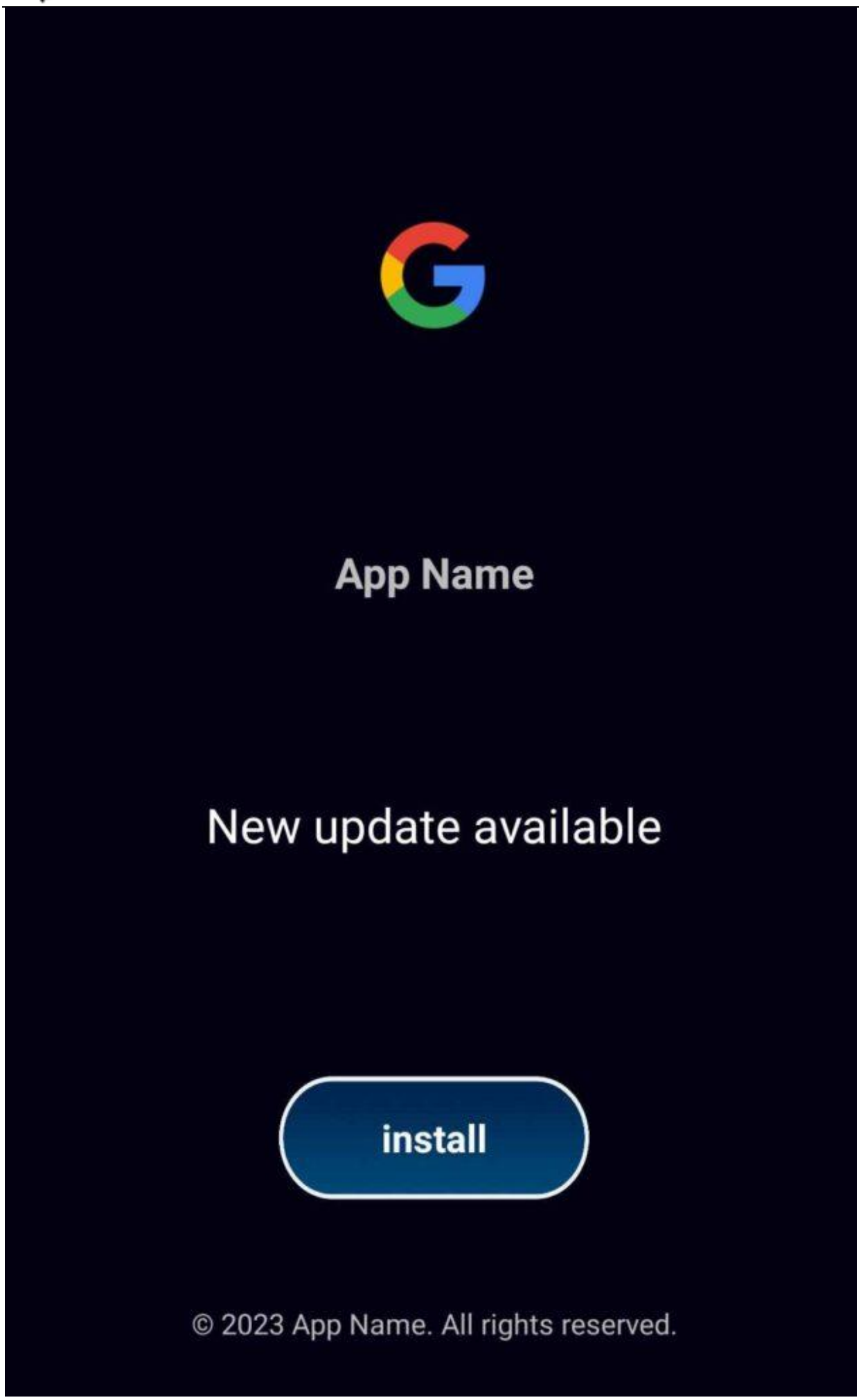
Đang mở sản phẩm,

xin vui lòng chờ đợi

GoldDigger displays a fake splash screen to its victim (in Vietnamese), followed by a request to enable the Accessibility service

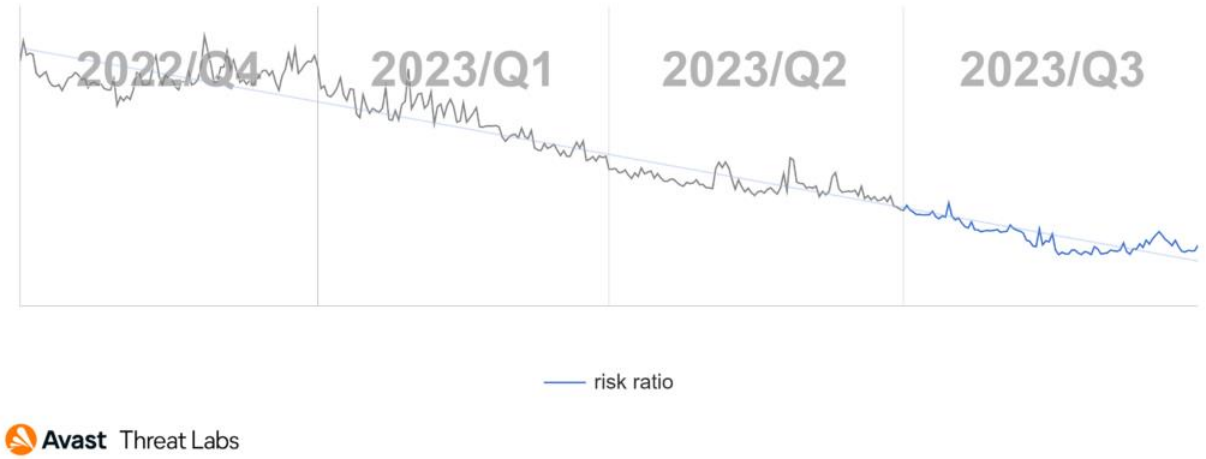
In an unusual twist, SpyNote has further evolved to the point of breaching into the banking sphere. Recent samples that we have observed are starting to use the spy features of this strain to extract 2FA messages as well as banking credentials and logins. Spreading through smishing and actual phone calls, victims are encouraged to update to a latest version of their banking application, which unfortunately is the SpyNote malware. This version of SpyNote uses the Accessibility service to key log victim's entries, record the screen and extract confidential information. It also features a defense module that is intended to prevent its removal. As mentioned in previous quarterly reports, we are seeing more spyware strains being re-used in the banking sphere and we anticipate this merging of strains will continue going forward.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55



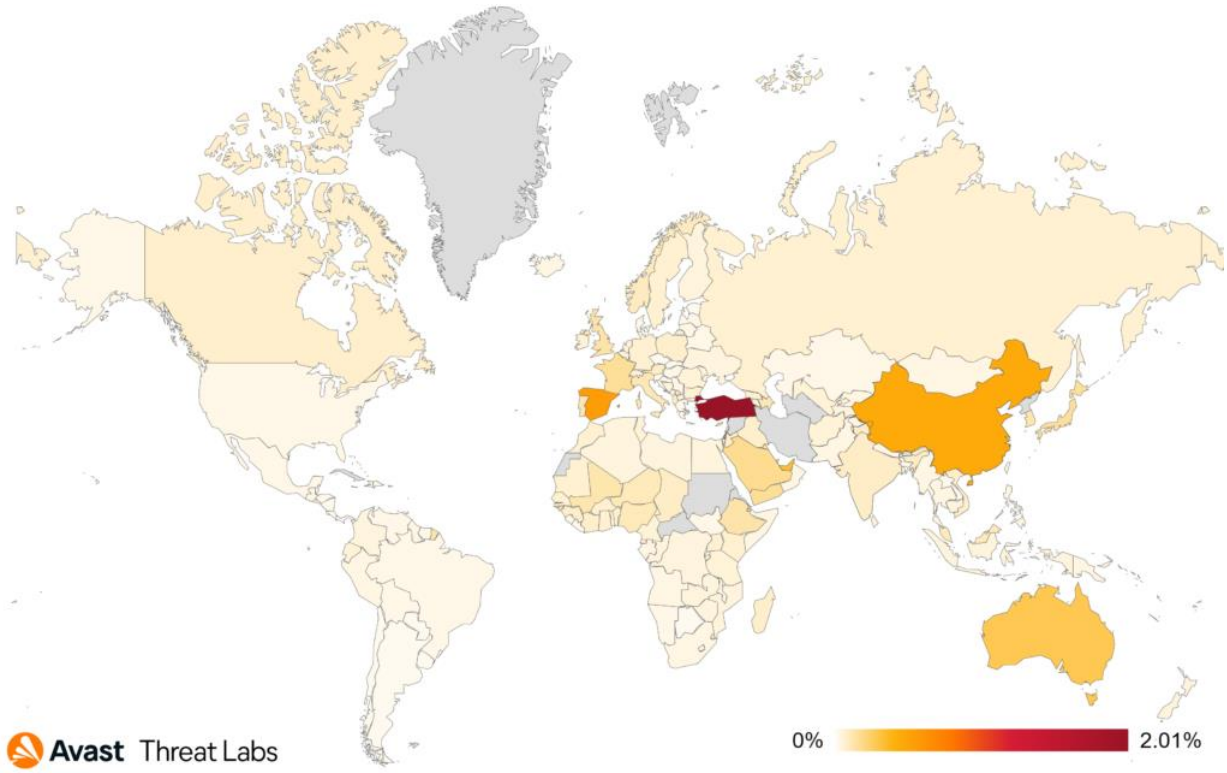
An unfinished SpyNote sample displays a fake update message that downloads further malicious APKs

Despite continued activity, updated strains and new bankers entering the market, we observe a steady decline in attacked users for several quarters in a row. We estimate that this is due to threat actors using more tailored approaches as of late as we observe less widespread SMS campaigns that were signature of FluBot and others a few quarters ago.



Global risk ratio of mobile bankers in Q4/2022-Q3/2023

Turkey continues to hold top place with the most protected users, closely followed by Spain, France, and the UK. Most of the banker focus appears to be on Europe, with a few exceptions such as Brazil, Japan, and Australia.



Global risk ratio for mobile bankers in Q3/2023

Spyware Telegram Mods Are on the Rise

Spyware is used to spy on unsuspecting victims with the intent of extracting personal information such as messages, photos, location, or login details. It uses fake adverts, phishing messages, and modifications of popular applications to spread and harvest user information. State backed commercial spyware is becoming more prevalent and is used to target individuals with 0-day exploits.

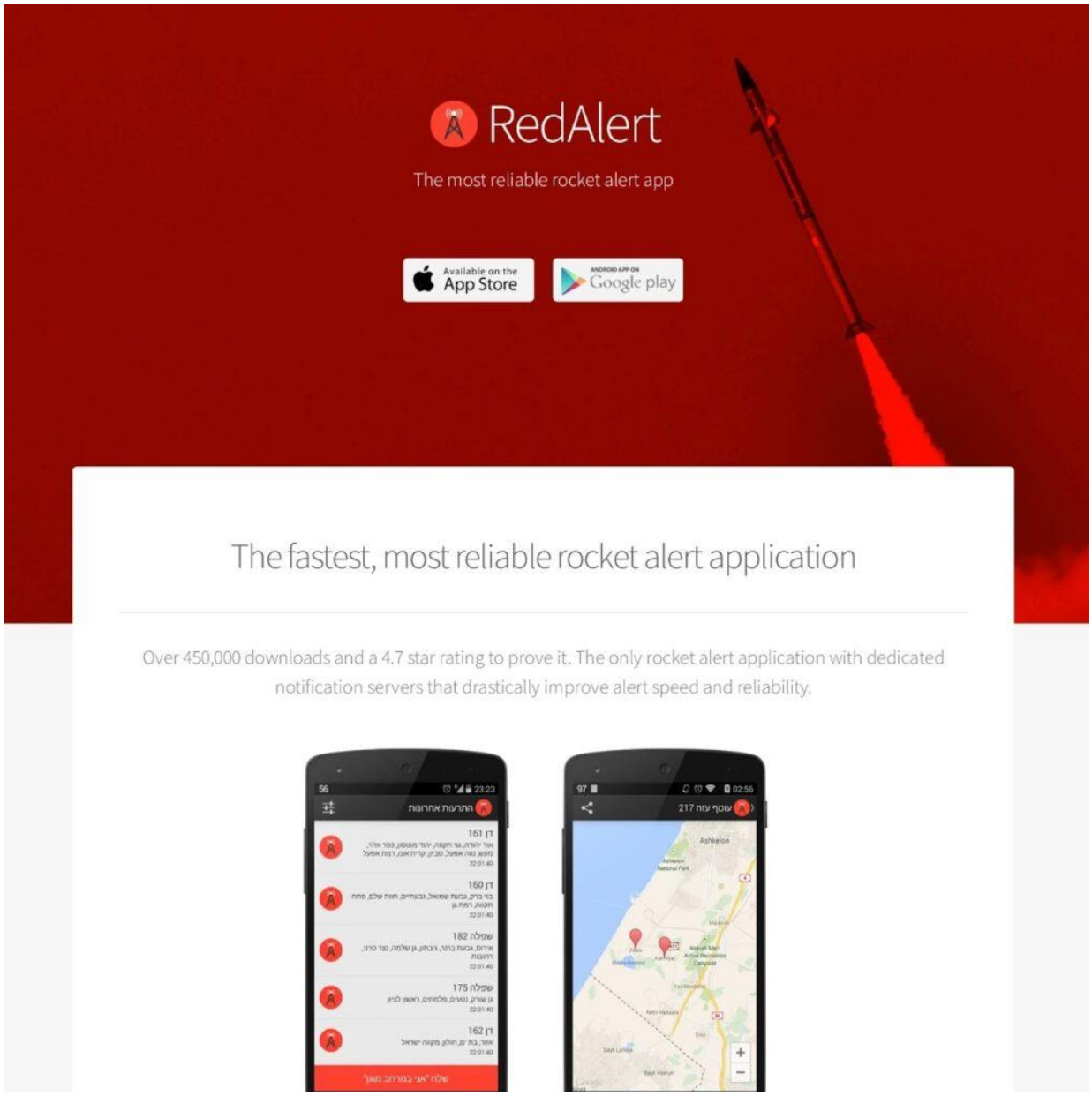
Spyware presence has slightly declined this quarter as Spymax maintains its top spot among the spyware strains with SexInfoSteal and FaceStealer trailing closely behind. New additions to the spyware family this quarter include several new trojanized modifications of popular messenger applications and SpyNote making another appearance. We note the spread of a fake spyware missile alert app in Israel and Spyloans continue their reign as several new samples have been spotted on the PlayStore.

Another version of SpyNote/Spymax was used as part of a short campaign targeting users in Japan with fake SMS messages about unpaid utility or water bills. Containing a sense of urgency, these messages led victims to a series of phishing sites which downloaded the SpyNote onto their devices. Once installed, the malware would direct users to open settings and enable the accessibility service to allow it install further malware and hide itself on the device. It then spied on victim's personal data and was able to access authenticator apps on the device and steal social media credentials.

```
yr.privMap = new HashMap();
yr.oppoPwd = "on";
yr.usrmode = "auto";
yr.PRMSV = "ST_CMA";
yr.OPPO_SHOWABLE = 0;
yr.verifyOppo = "on";
yr.verifyOneplus = "on";
yr.verifyRealme = "on";
yr.verifyXiaomi = "on";
yr.verifyHuawei = "on";
yr.verifySamsung = "on";
yr.verifyVivo = "on";
yr.verifyGoogle = "on";
yr.hookUninstall = "off";
yr.hookHighGrant = "off";
yr.hookNotification = "on";
yr.hookRecents = "off";
yr.hookAccessibility = "on";
yr.hookResetDev = "off";
yr.hookAppStore = "off";
yr.hookEngine = "off";
yr.hookOpenmanager = "off";
yr.hookSysmanager = "off";
yr.grantTextFontSize = "14";
yr.grantSubTextFontSize = "13";
yr.LOOPNOTIFY = "on";
yr.isHookUNS = false;
yr.isHookGrant = false;
yr.isHookNotification = false;
yr.isHookRecents = false;
yr.isHookAccess = false;
yr.settingHooks();
```

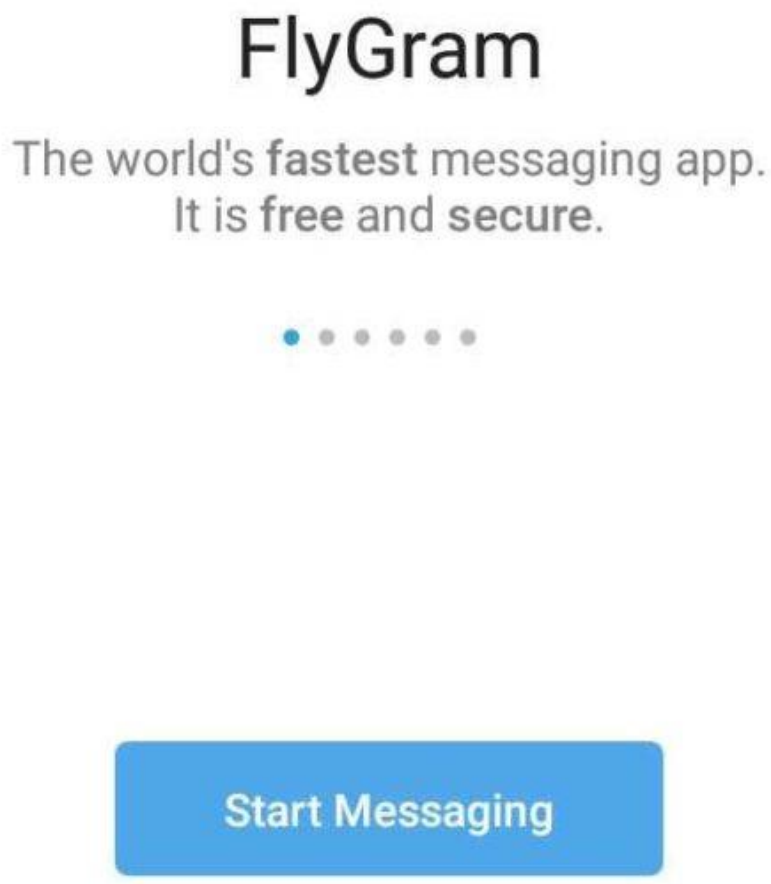
Konfiguration enthält verschiedene Einstellungen und Prüfungen, z. B. die Aktivierung der Barrierefreiheit

Im Zusammenhang mit der jüngsten Eskalation der Situation zwischen Israel und Palästina ist es erwähnenswert, Alarmstufe Rot“ dass über eine Phishing-Website eine Spyware-App zur Raketenwarnung „ verbreitet wurde. Die Original-App wird von vielen in Israel zur Überwachung von Raketenwarnungen genutzt. Die gefälschte Spyware-App Red Alert enthielt identische Funktionen mit zusätzlichen Fähigkeiten, die es ihr ermöglichten, ihre Opfer auszuspionieren. Dazu gehörte unter anderem das Extrahieren des Anrufprotokolls, der SMS-Listen, des Standorts und der E-Mails. Die Malware verfügt außerdem über Anti-Debugging und Anti-Emulation, die versuchen, die Erkennung zu verhindern. Auch wenn dies nicht dokumentiert ist, ist es möglich, dass diese Malware auch zur Übermittlung gefälschter Warnmeldungen verwendet werden könnte, wie es bei anderen gehackten Raketenwarn-Apps der Fall war.



Phishing-Site, die sich als die ursprüngliche RedAlert-Raketenwarn-Website ausgibt und die Spyware-Payload herunterlädt

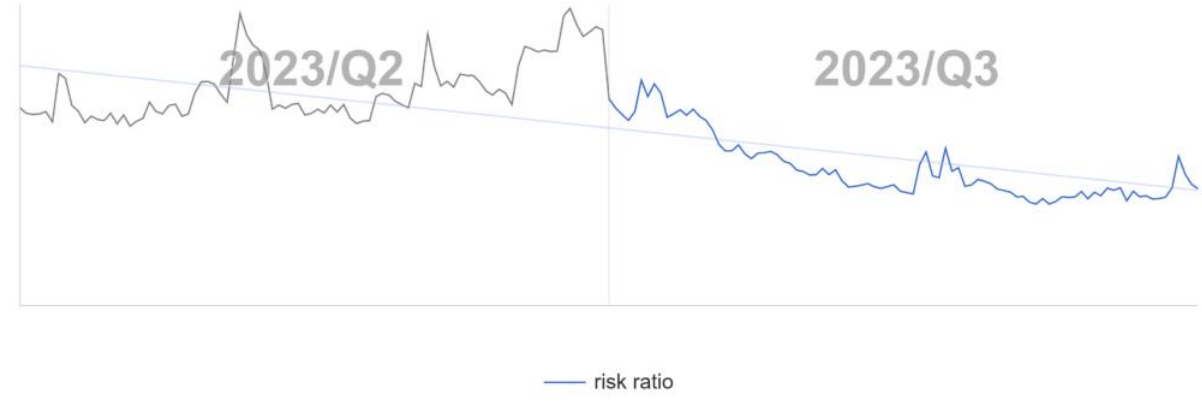
Wie in den vergangenen Quartalsberichten erwähnt, werden Mods für WhatsApp, Telegram und Signal immer beliebter für Bedrohungsakteure. Wir beobachten einen weiteren Fall von trojanisierten Telegram-Mods, die im PlayStore entdeckt wurden, diesmal gegen chinesischsprachige Opfer. Diese Version sieht auf den ersten Blick wie die Telegram-App aus, sammelt jedoch im Hintergrund Benutzerinformationen, Nachrichten, Anrufe und Kontaktlisten. Diese werden dann an einen Cloud-Dienst exfiltriert, um von böswilligen Akteuren weiter genutzt zu werden. In ähnlicher Weise BadBazaar- wurden Samples über trojanisierte Signal- und Telegram-Apps verbreitet. Diese Sorte nutzt gefälschte Websites, um Opfer anzulocken, und zielt offenbar auf die uigurische Bevölkerung ab. Es enthält einen ähnlichen Spyware-Funktionsumfang wie die trojanisierten Telegram-Mods. Diese böswilligen Änderungen bleiben bestehen und Benutzern wird empfohlen, Änderungen an beliebten Messaging-Apps zu vermeiden.



Begrüßungsbildschirm des gefälschten FlyGram-Mods, der BadBazaar-Spyware enthält

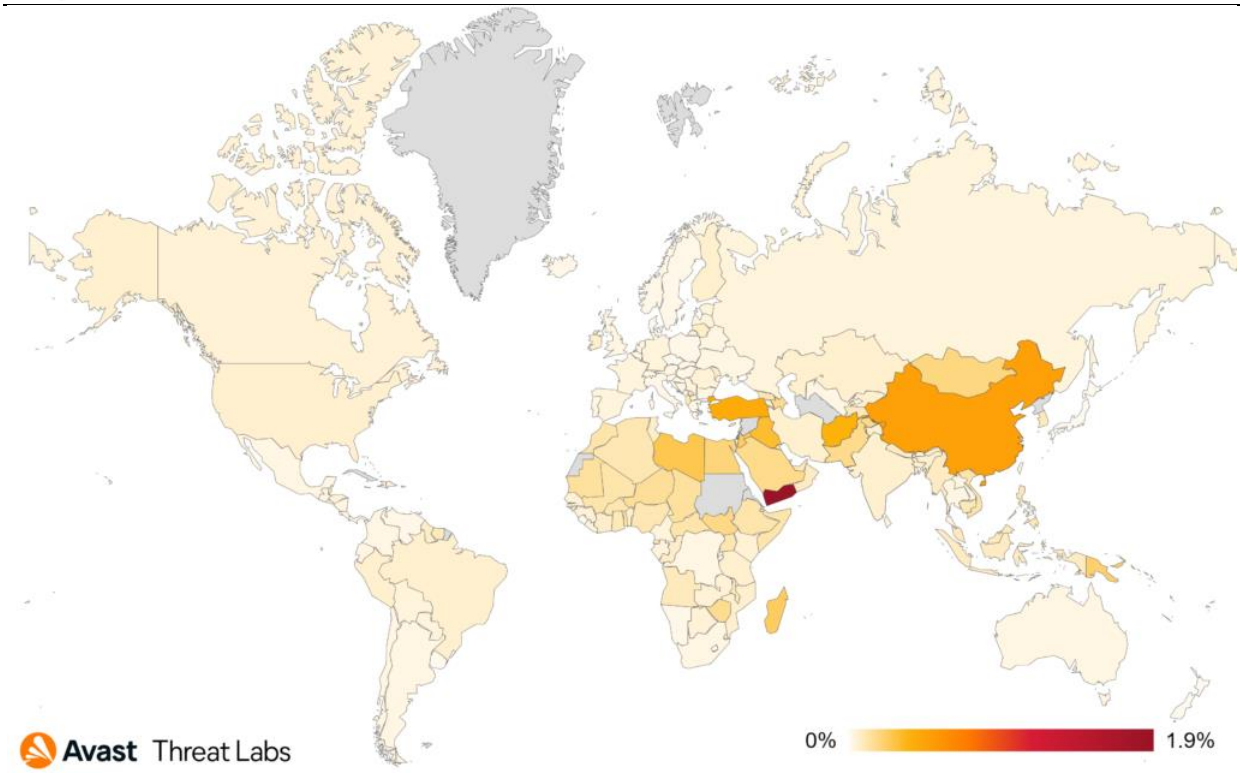
Spyloan-Anwendungen verbreiten sich weiterhin im PlayStore. Wie Zimperium berichtet , bleiben diese Apps größtenteils unverändert und bieten Kredite an ahnungslose Opfer in verschiedenen asiatischen und südamerikanischen Ländern. Sobald der Benutzer die Anwendung installiert, fordert er unter dem Deckmantel einer Bonitätsprüfung verschiedene invasive Berechtigungen an. Wenn das Opfer dies zulässt, sammeln die Akteure hinter den Spionagekrediten Opferdaten wie Nachrichten, Kontaktlisten und Fotos, um nur einige zu nennen. Diese werden dann verwendet, um Opfer zu erpressen, sodass sie häufig mehr als den vereinbarten Betrag zahlen, und diese Belästigungen können auch nach der Begleichung der Schulden anhalten. Benutzern wird empfohlen, inoffizielle Kreditquellen zu meiden, um diese Art der Erpressung zu vermeiden.

Dieses Quartal bringt einen leichten Rückgang der Verbreitung von Spyware im Mobilfunksektor mit sich. Während sich mehrere Arten bösartiger Mods in den PlayStore eingeschlichen haben, beobachten wir in diesem Quartal insgesamt einen Rückgang der Aktivität und Verbreitung von Spyware.



Globales Risikoverhältnis von mobiler Spyware im 2. Quartal 2023 und im 3. Quartal 2023

Brasilien weist in diesem Quartal weiterhin die höchste Anzahl geschützter Benutzer auf, gefolgt von der Türkei, den USA und Indien. Jemen hat im Vergleich zum Rest der Welt das höchste Risiko, auf mobile Malware zu stoßen.



Global risk ratio for mobile spyware in Q3/2023

Jakub Vávra, Malware Analyst

Acknowledgements / Credits

Malware researchers

Adolf Středa
Alexej Savčin
Bohumír Fajt
Branislav Kramár
David Álvarez
Igor Morgenstern
Jakub Křoustek
Jakub Vávra
Jan Rubín
Jan Vojtěšek
Ladislav Zezula
Luigino Camastra
Luis Corrons
Martin Chlumecký
Matěj Krčma
Michal Salát
Ondřej Mokoš

Data analysts

Pavol Plaskoň
Filip Husák
Lukáš Zobal

Communications

Brittany Posey
Emma McGowan

Tagged asdesktop, malware, mobile, report, risk, threats

Further reading

PC

Rhysida Ransomware Technical Analysis

6 min read

Technical analysis of Rhysida Ransomware family that emerged in the Q2 of 2023

PC

Love-GPT: How “single ladies” looking for your data upped their game with ChatGPT

12 min read

Love-GPT is a tool that provides vast functionality over several different dating platforms, providing the capability to create fake accounts, interact with victims, anonymize the access, and more. It also uses ChatGPT, to achieve its goals.

DECODED .io

Kategorien

- Veranstaltungen
- IoT
- Handy, Mobiltelefon
- Netzwerk
- Sonstiges/Forschung
- PC
- Berichte
- Nicht kategorisiert

Stichworte

Analyse Android APT Backdoor Botnet Brasilien Kryptowährung Cryptomining CSRF DDOs Decryptor Decryptors Desktop DirtyMoe DNS-Hijack Fake - Ghostdns Google Play Store HW IoT - Malware Mobile Verschleierung P-Code Phishing Ransomware Rattenbericht Exploit Forschung Risikoumkehr Dropper Rootkit Router Sicherheitsserie App Spyware Stealer Takedown Bedrohung – Informationen Bedrohungen VB- Sicherheitslücke Wurm

kürzliche Posts

- Avast-Bedrohungsbericht Q3/2023
- Rhysida Ransomware Technische Analyse
- Love-GPT: How “single ladies” looking for your data upped their game with ChatGPT
- Insights into the AI-based cyber threat landscape
- Avast Q2/2023 Threat Report

Archive

- November 2023
- October 2023
- September 2023
- August 2023
- July 2023
- June 2023
- May 2023
- April 2023
- February 2023
- January 2023
- December 2022
- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- December 2021
- November 2021
- October 2021
- September 2021
- August 2021
- July 2021
- June 2021
- May 2021
- April 2021
- March 2021

- February 2021
- December 2020
- November 2020
- October 2020
- September 2020
- August 2020
- June 2020
- May 2020
- April 2020
- December 2019
- September 2019
- August 2019
- July 2019
- April 2019
- March 2019
- February 2019
- January 2019
- August 2018
- January 2018
- October 2017

Meta

- Log in
- Entries feed
- Comments feed
- WordPress.org

Quelle: https://decoded.avast.io/threatresearch/avast-q3-2023-threat-report/