Bitdefender Threat Debrief | November 2021

The Bitdefender Threat Debrief (BDTD) is a monthly series analyzing threat news, trends, and research from the previous month. You can find all previous debriefs here.

Highlight of the month: Introducing Android report (H2)

We keep adding new cybersecurity research to our monthly threat debrief! Last month, we added a homograph phishing report focused on top spoofed domains and the most common targets. This month, we introduce a section focused exclusively on mobile threats targeting Android.

Our mobile research is timely as the European Union considers a draft of the Digital Markets Act. Under the new Act, phone makers are required to allow third-party software from unofficial app stores to be supported on all platforms. While the Digital Markets Act will probably not become law prior to 2023, it is an important security topic that has been getting more attention recently and something to keep close watch on. We have previously seen advanced malware on Android – if you want to learn more about this topic, we recommend a white paper Uprooting Mandrake: The Story of an advanced Android Spyware Framework That Went Undetected for 4 Years.

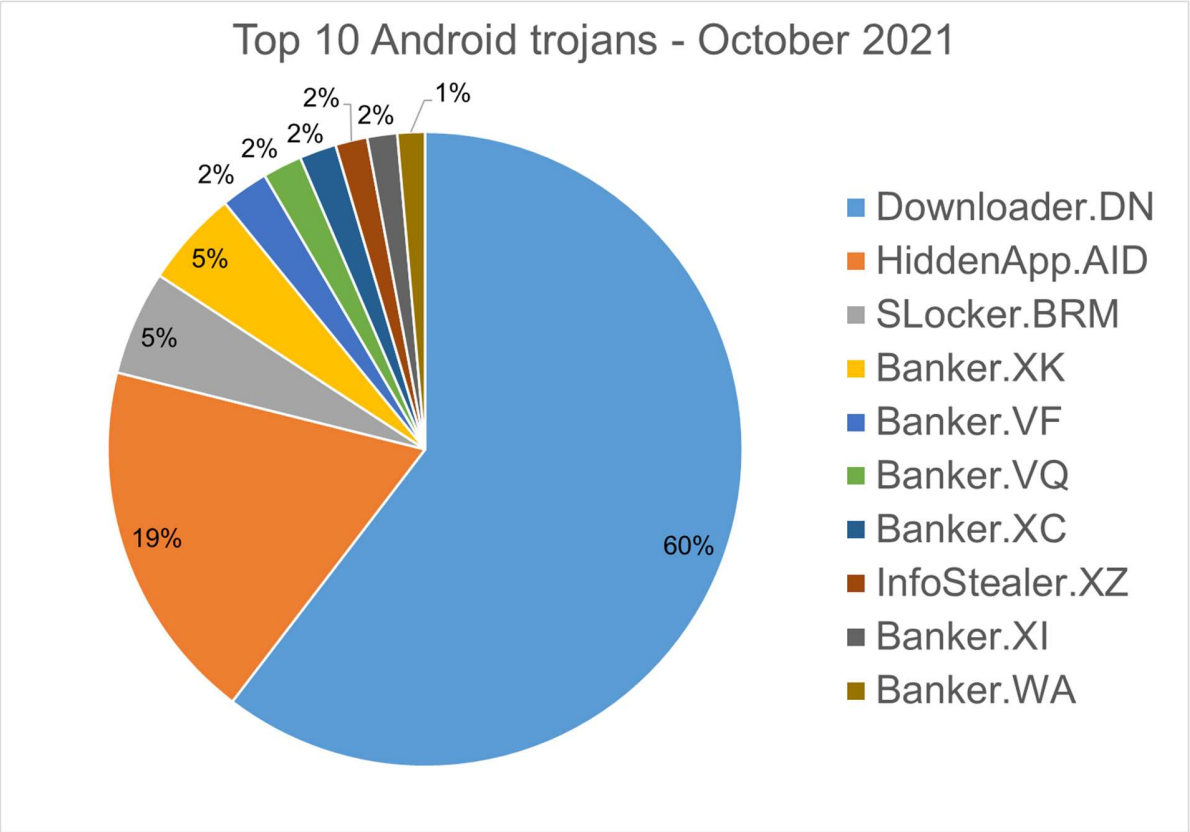
Defense-in-depth is an important concept for all aspects of cybersecurity, including mobile. In this report, we present data from Bitdefender Mobile Security telemetry (available for Android and iOS platforms). Many attacks rely on social engineering techniques not blocked by gatekeeping measures of popular application stores – smartphones and tablets are essentially small-factor computers and require protection as well.

Bitdefender Mobile Security blocks a malware app

In this issue, we look at the top 10 trojans on Android and findings from our mobile scam alert protection feature.

Top 10 Android trojans (H3)

Below are the top 10 trojans that we have seen in our telemetry for October 2021.



Android.Trojan.Downloader.DN – Repacked applications taken from Google App Store and bundled with aggressive adware. Some adware downloads other malware variants.

Android.Trojan.HiddenApp.AID - Aggressive adware that impersonates adblock applications. When run for the first time, it asks permission to display on top of other apps. With this permission, the application can hide from the launcher.

Android.Trojan.SLocker.BRM - Applications that block access to devices by displaying a screen that appears over every window, so that the user is frozen. This is a simplistic version of mobile ransomware.

Android.Trojan.Banker.WT - Applications that impersonate legit apps (DHL, FedEx). When installed, it asks for accesibility permissions and once granted, will steal, collect and upload banking information to a command-and-control server (C&C) contact list.

Androi.Trojan.Banker VF, VP, XI - Polymorphic applications that impersonate legit apps (Google, Facebook, Sagawa Express ...). Once installed, it locates banking applications installed on the device and tries to download a trojanized version from the C&C server.

Android.Trojan.Banker.XK - Applications that impersonate Korean banking applications to record audio and video, collect sensitive information and upload it to a C&C server.

Top 10 Android malware URLs (H3)

The following is based on data from our scam alert feature that– detects link-based attacks delivered through messaging apps and notifications. Notifications are from communication applications such as WhatsApp, Telegram, Facebook Messenger, Twitter, Discord and others.

Sources column in the table below identifies where Bitdefender Mobile Security detected the malicious URL link. Ringbell ( ) represents a notification (most often from messaging application such as WhatsApp or Facebook Messenger), and two different icons represent incoming ( ) and outgoing ( ) text messages. Outgoing text messages are likely text messages utilizing social engineering techniques to convince a victim to forward message to other people.

URL	Status	Sources	Top Countries
https://dhani.onelink.me/zcy7/ffea724f	malware		
https://hermes.check-online-reschedule.com	phishing		
https://hermes.check-reschedule-online.com	phishing		
https://dhani.onelink.me/zcy7/23620ad7	malware		
https://myhermes.online-item-tracking.com	phishing		
basvuru.evde-uygun-internet.com	malware		
musicvideoz.biz	fraud		
https://myhermes.tracking-online-item.com	phishing		
https://dliscord.com/xgcs7cgt2sdfof82	malware phishing		
https://dhani.onelink.me/zcy7/8a2174a5	malware		

We include the list of IOCs at the end of this report.

Homograph Phishing Report (H2)

Here we focus on homograph attacks that abuse international domain names (IDN). Threat actors create international domain names that spoofs a target domain name. When we talk about “target” of IDN homograph phishing attacks, we refer to the domain that threat actors are trying to impersonate. You can read more about this type of attacks in our previous report.

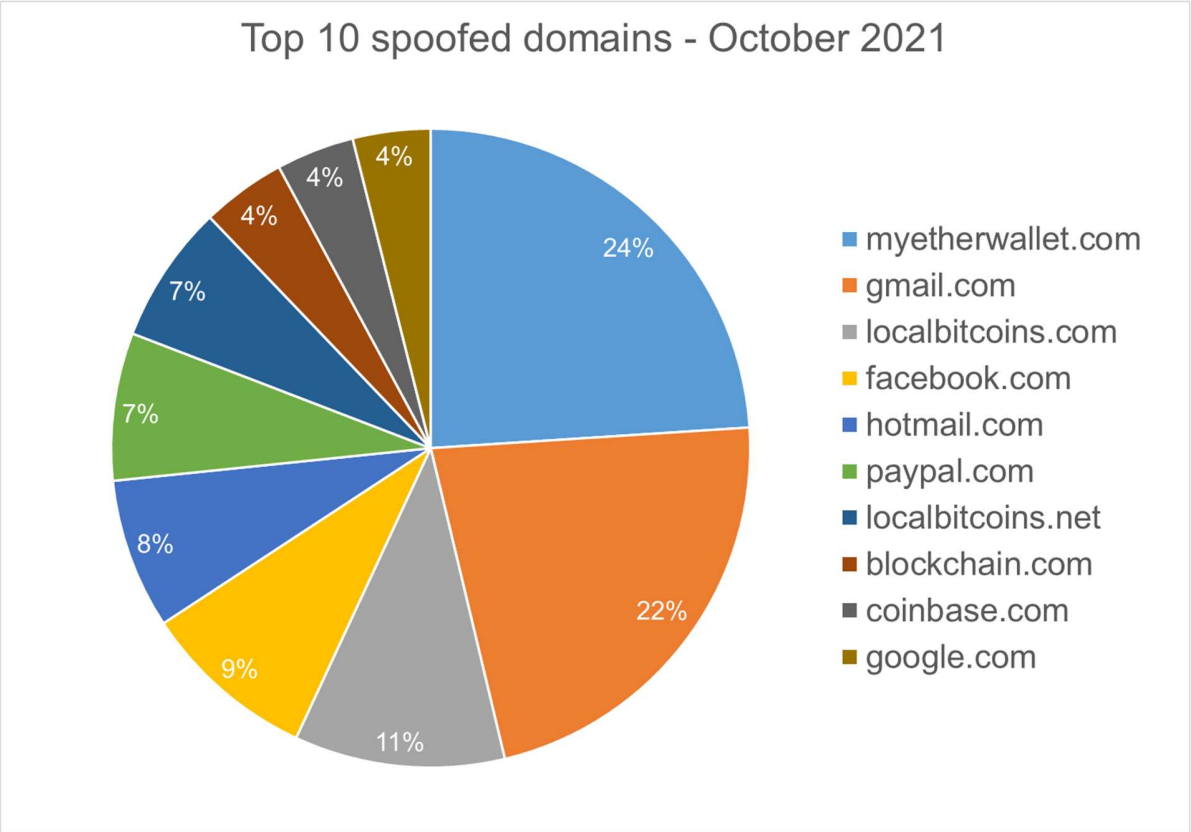
When we analyzed and categorized targets of IDN spoofing attacks, three categories stood out from the rest. The first is credential stealing targeting cryptocurrency exchanges and banks. It's the quickest most direct way to monetize an attack, so it is not surprising to see them at the top of the list. Social media and consumer domains (Gmail, Hotmail, PayPal, Amazon etc.) are useful for credential harvesting which fetch premium prices on the dark web. Threat actors collect and save logon credentials and either use them to launch another attack (for example to reset password for a more sensitive site) or sell them to other criminals.

These three categories combined are making over 65% of the detected spoofing attacks.

1. Cryptocurrencies (34.82%)
2. Banks (15.36%)
3. Social Networks (14.96%)

1 in 10 (12%) homograph domains are using HTTPS encryption. The use of HTTPS helps threat actors avoid detection with network-based security controls, but more importantly, spoofed sites appear legitimate (green padlock).

Below is the list of the top 10 most common targets for phishing sites.



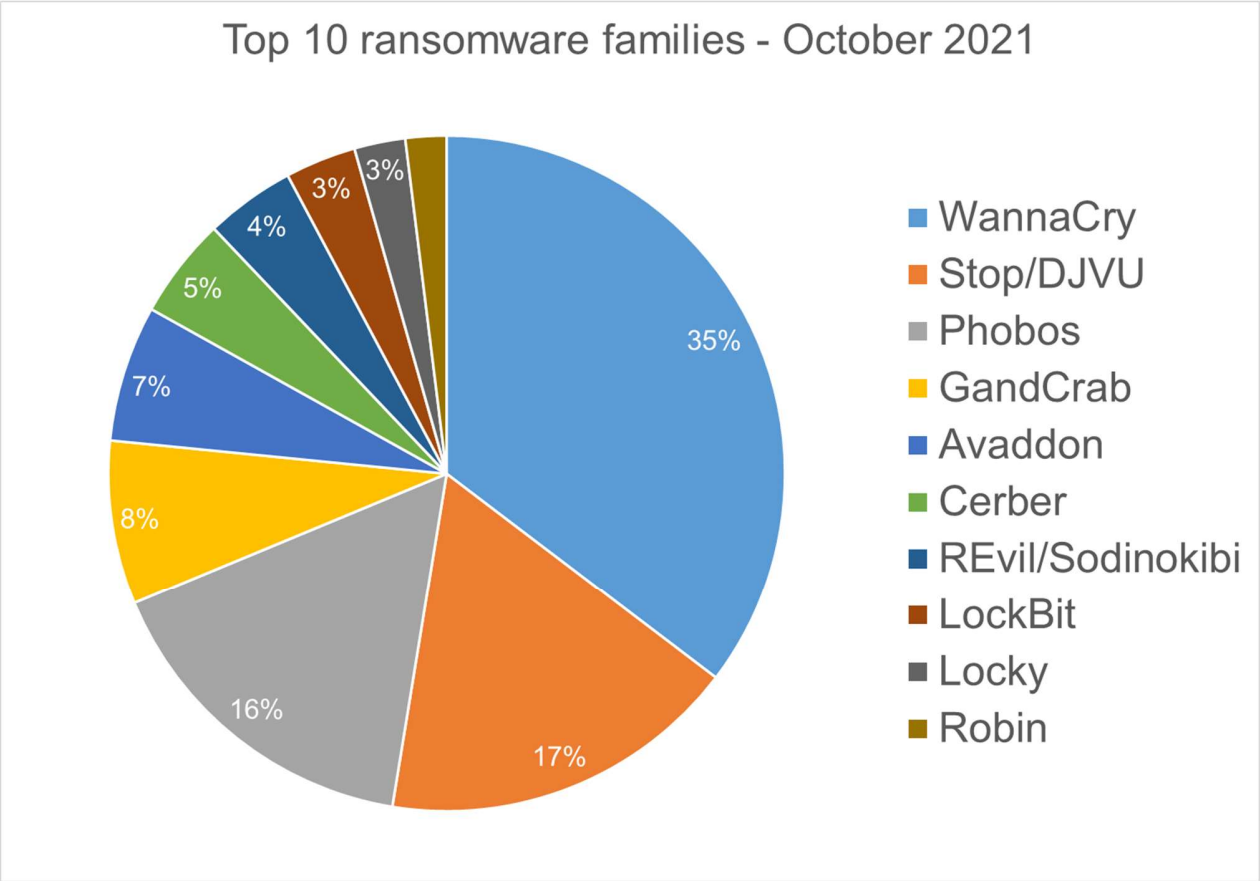
Ransomware Report (H2)

Spear phishing attacks are often used as an initial attack vector. Ransomware infection is often the final stage of the same kill chain. For this report, we analyzed malware detections collected in October 2021 from our static anti-malware engines. Note: we only count total cases, not how monetarily significant the impact of infection is. Opportunistic adversaries and Ransomware-as-a-Service (RaaS) groups represent a higher percentage compared to groups that are more selective about their targets, since they prefer more volume instead of higher value.

When looking at this data, remember these are ransomware detections, not infections. Companies in the technology industry rank at the top of our list with the most detections, while non-profit organizations are trailing at the end. Detection rates vary based on technologies in place and security maturity.

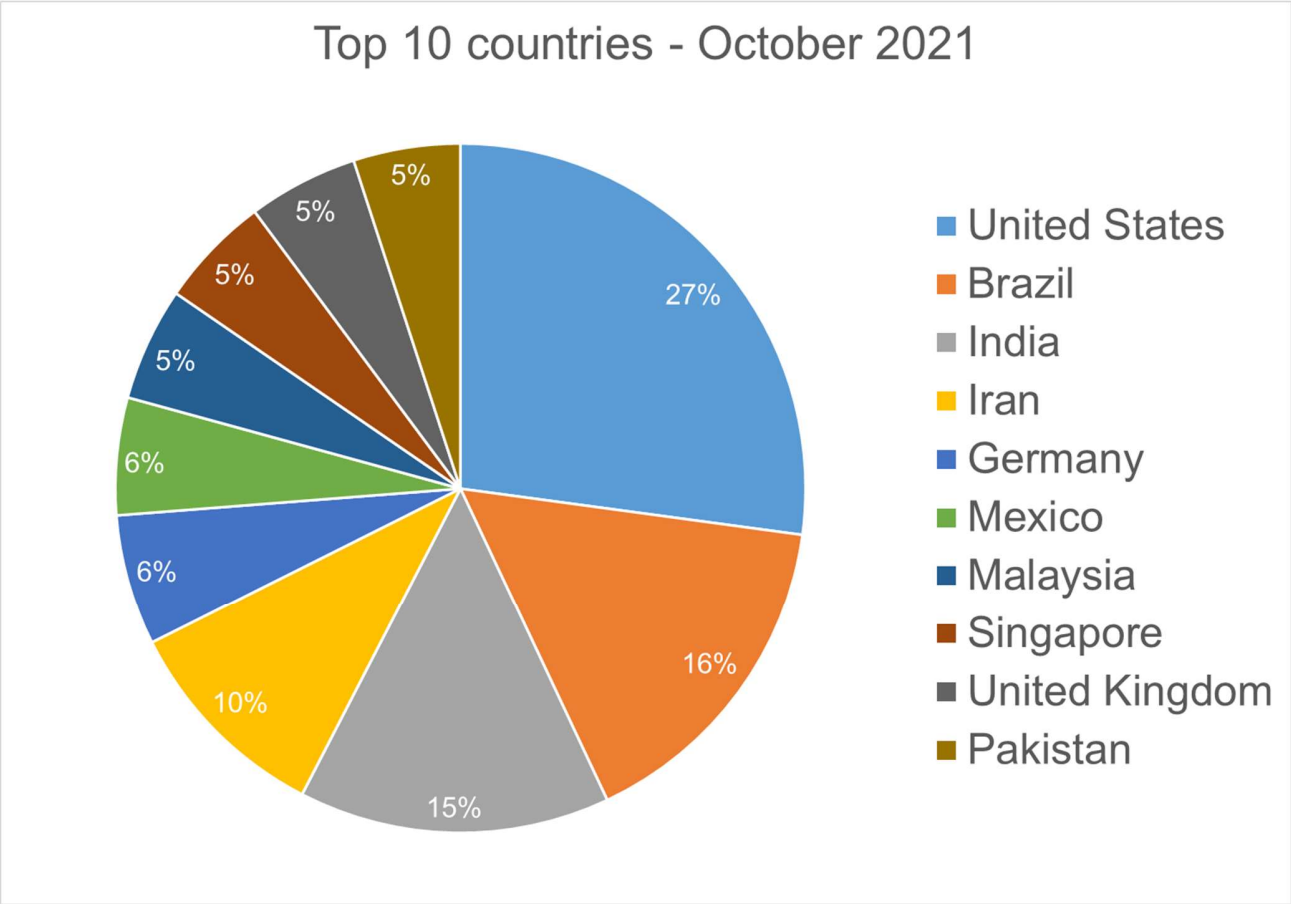
Top 10 Ransomware Families (H3)

For this report, we analyzed **13.3 million malware detections** from October 1st to October 31st. In total, we identified **233 ransomware families**. Number of detected ransomware families can vary each month, depending on the current ransomware campaigns in different countries.



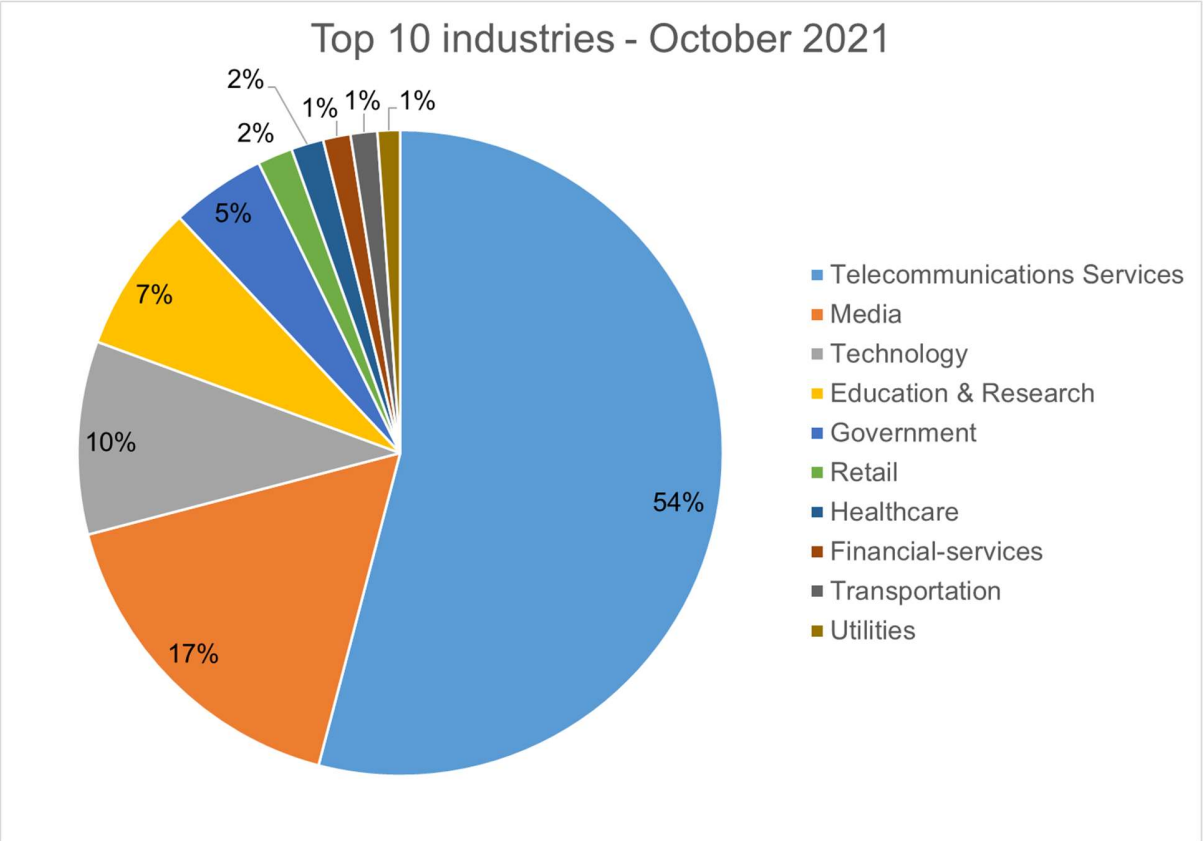
Top 10 Countries (H3)

In total, we detected ransomware from 167 countries in our dataset this month. Ransomware continues to be a threat that touches almost the entire world. Below is a list of the top 10 countries most impacted by ransomware. Most ransomware attacks continue to be opportunistic, and the size of population is correlated to the number of detections.



Top 10 Industries (H3)

For our dataset, we have been able to assign almost 40% of detections to specific industries. Telecommunications services are particularly high as their customers are included within the detections.



From our Petri digi-dish (h2)

In this section, we highlight other key research from Bitdefender Labs:

- Digitally signed rootkits are back. For the past few months, Bitdefender researchers have seen a surge in malicious drivers with valid digital signatures issued by Microsoft through the WHQL signing process. Read more in our research white paper Digitally-Signed Rootkits are Back – A Look at FiveSys and Companions.

Summary (H2)

In this issue of BDTD, we added new research on mobile threats. Modern smartphones require high-level security, yet many are still under the assumption security is already built into phones and/or cybercriminals target mobile devices less often. Bitdefender released a study in October on cybersecurity and online behaviors and found 35% of users don't use antivirus on their phones yet, 61% experienced at least one mobile threat in the last 12 months. Additionally, the notion of requiring Apple to allow application sideloading (opening the flood gates to cybercriminals), makes the topic of mobile security evermore pressing.

To stay ahead of attackers, keep up to date with the latest threats and best practices. Subscribe to the Business Insights blog, follow us on Twitter, and don't miss the next BDTD for November .

We hope you have found this BDTD report interesting. Leave us a comment and let us know what you think.

Indicators of Compromise (H2)

An up-to-date and complete list of indicators of compromise is available to Bitdefender Advanced Threat Intelligence users. The currently known indicators of compromise can be found in the table below.

URLs
https://dhani.onelink[.]me/zcy7/ffea724f
https://hermes.check-online-reschedule[.]com
https://hermes.check-reschedule-online[.]com
https://dhani.onelink[.]me/zcy7/23620ad7
https://dhani.onelink[.]me/zcy7/ffea724f
https://myhermes.online-item-tracking[.]com
basvuru.evde-uygun-internet[.]com
Musicvideoz[.]biz
https://myhermes.tracking-online-item[.]com
https://dliscord[.]com/xGCs7cGt2sdFOf82

About Bitdefender Threat Debrief (H2)

Bitdefender provides cybersecurity solutions and advanced threat protection to hundreds of millions of endpoints worldwide. More than 150 technology brands have licensed and added Bitdefender technology to their product or service offerings. This vast OEM ecosystem complements telemetry data already collected from our business and consumer solutions. To give you some idea of the scale, Bitdefender Labs discover 400+ new threats each minute and validate 30 billion threat queries daily. This gives us one of the industry's most extensive real-time view of the evolving threat landscape.

We would like to thank bitdefenders Alin Damian, Mihai Leonte, Ioan Marculet, Andrei Mogage, Ioan Stan, Marius Tivadar, and Horia Zegheru (sorted alphabetically) for their help with putting this report together.