ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 5, Issue 19

B-2025-09-25b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

September 25, 2025

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 10:30 AM (EDT) on September 25, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 5, Issue 19

| Cyberattacks on European Airports Reveal Contagion Risk

Over the weekend of September 19–21, 2025, a cyberattack caused widespread operational disruption at major European airports, resulting in a host of flight cancellations and delays. The attack reportedly targeted the Multi-User System Environment (MUSE) passenger processing software provided by Collins Aerospace, forcing airlines and ground services to revert to manual check-in and boarding procedures.[1]

- On September 22, 2025, the European Union Agency for Cybersecurity (ENISA) confirmed that the cause of the disruption was a ransomware attack but did not disclose the threat actor behind it.[2]
- Collins Aerospace is a U.S.-based aviation and defense technology company—with a global presence at more than 170 airports—that offers solutions for passenger processing and facilitation, airport operations, and baggage management.[3]

[1] hXXps://www.csoonline[.]com/article/4060804/european-airports-continue-to-crawl-after-a-cyberattack-on-collins-muse-systems.html

[2] hXXps://www.aa[.]com[.]tr/en/europe/eu-cybersecurity-agency-confirms-ransomware-attack-behind-airport-disruptions/3694832

[3] hXXps://www.collinsaerospace[.]com/what-we-do

In a statement to *Reuters*, RTX Corporation (formerly Raytheon Technologies Corporation), the parent company of Collins Aerospace, stated that it was aware of the cyber disruptions at certain airports without specifying which ones; however, several airports in the region have since reported being affected by the software disruptions. Heathrow Airport in London (Europe's busiest airport), Brussels Airport, Berlin Brandenburg Airport, Dublin Airport, and Cork Airport have also revealed varying degrees of impact.[4]

In previous systems, each airline managed its own dedicated service area in an airport, making access singular and contained to the airline itself. However, in recent years, concerns regarding efficiency have caused several airports to shift toward newer systems like MUSE, a shared-use platform that integrates passenger records, baggage details, and security requirements into one digital platform used across airlines to enable dynamic desks and gates within airports.[5]

- This change underpins the increased likelihood of vulnerabilities to European aviation, as an attack on one entity could impact multiple airports, unlike the previous system, wherein threat actors would only be able to target airlines individually.
- As a result of MUSE's compromise, every airline in an impacted airport likely could not access their shared digital framework, forcing them to rely on often cumbersome and time-consuming manual check-ins.
- Due to the check-in disruptions, several airports experienced subsequent delays and flight cancellations, which are likely to persist if airlines continue to experience prolonged digital limitations.

As of writing, no threat actor has claimed responsibility for the attack. The attribution details—such as the ransomware strain or the threat actor responsible—have not yet been made public, and it remains unclear whether a third-party vendor or Collins Aerospace itself was targeted. There is currently no evidence to suggest a data breach

[4] hXXps://www.reuters[.]com/en/cyberattack-causes-flight-delays-cancellations-brussels-airport-2025-09-20/

[5] hXXps://www.techtimes[.]com/articles/312010/20250920/software-behind-europes-check-chaos-what-muse-why-it-matters.html

has taken place or that passenger data has been compromised; however, digital forensic analysis is reportedly ongoing.[6]

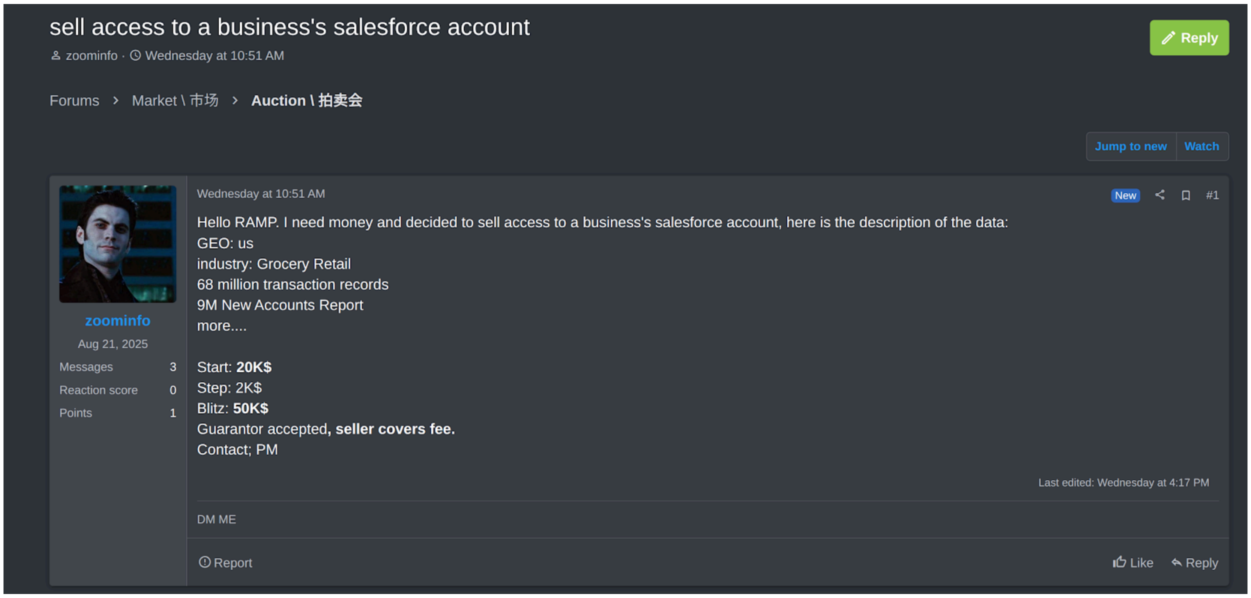
This attack highlights a critical vulnerability in the IT infrastructure used in the aviation industry, especially where third-party systems support multiple airports and airlines. The airline industry likely faces significant pressure to quickly meet ransomware demands, as customer satisfaction and maintaining scheduled flight times are crucial to its business model. It is likely that airport authorities and affected airlines will face pressure to reassess cyber resilience standards and supply chain risk management as a result of this attack.

Salesforce Business Account Advertised for Sale

On September 9, 2025, an actor known as “zoominfo” advertised unauthorized access to an unnamed Salesforce business account on the primarily Russian-language dark web forum RAMP. According to the actor, the account and data allegedly belongs to an undisclosed U.S.-based grocery retailer business with USD 68 million in transaction records and USD 9 million in its most recent accounts report.

- The starting price is listed at USD 20,000, with bid increments of USD 2,000; however, an interested buyer can immediately purchase the access—without bidding—for USD 50,000.
- The actor states that purchases can be made via escrow or middleman services, which are likely offered to increase zoominfo’s credibility and the perceived security of the purchase for potential buyers.

[6] hXXps://www.reuters[.]com/business/aerospace-defense/european-airports-race-fix-check-in-glitch-after-hacking-disruption-2025-09-21/



sell access to a business's salesforce account

zoominfo · Wednesday at 10:51 AM

zoominfo
Aug 21, 2025

Wednesday at 10:51 AM

Hello RAMP. I need money and decided to sell access to a business's salesforce account, here is the description of the data:
GEO: us
industry: Grocery Retail
68 million transaction records
9M New Accounts Report
more....

Start: **20K$**
Step: 2K$
Blitz: **50K$**
Guarantor accepted**, seller covers fee.**
Contact; PM

Last edited: Wednesday at 4:17 PM

DM ME

zoominfo's advertisement on RAMP

Source: ZeroFox Intelligence

The actor zoominfo first appeared on the forum on August 21, 2025, and has zero reaction scores; as a newly registered account with limited presence on the platform, it is likely that potential buyers will be cautious about this advertisement. As such, ZeroFox cannot determine the legitimacy of the untested actor's claims at this time.

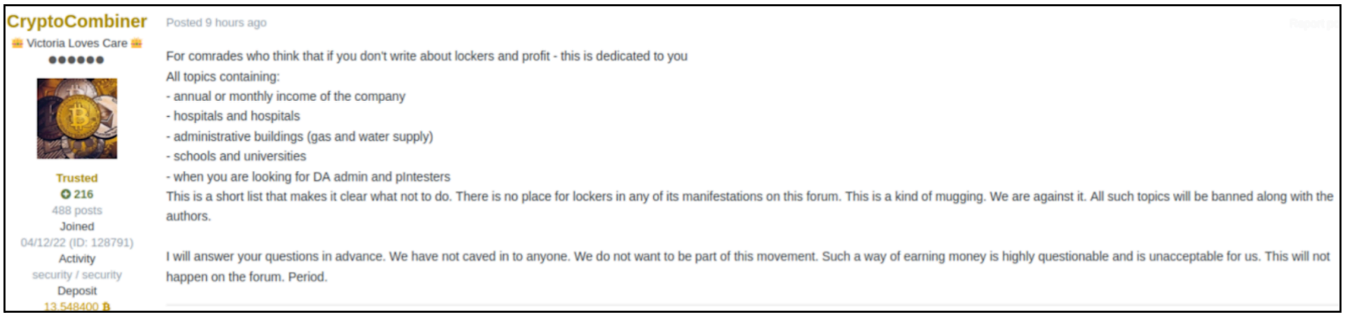
- Additionally, while this type of offer is common on the dark web, the extremely high price for such access is notably uncommon. There is a roughly even chance this signifies the actor's inexperience, that it is a fraudulent offer, or that it is significantly overpriced due to the notoriety of the recent Salesforce breaches.

While the actor claims to have access to a Salesforce business account, zoominfo does not allude to the recent Salesforce breaches, nor is there any evidence to suggest that this alleged account is linked to the large-scale Salesforce breach; however, the possibility cannot entirely be ruled out. If the actor does possess full access to a business Salesforce account, that would very likely cause significant harm to the company and its customers.

New Trend Observed on Dark Web Forum

On September 8, 2025, the actor "CryptoCombiner" posted on the dark web forum Exploit, offering advice on what not to provide in advertisements to initial access brokers involved in cryptolockers campaigns, which are strictly prohibited on the forum.

- A cryptolocker campaign refers to a cybercrime operation that deploys a cryptolocker ransomware to infect victims' computers, encrypt their files, and demand a ransom payment (typically in cryptocurrency) in exchange for the decryption key.
- Ransomware campaigns have been prohibited on dark web forums Exploit and XSS since early 2022. This was mostly motivated by the DarkSide ransomware attack against Colonial Pipeline in May 2021, which garnered a lot of media and law enforcement (LE) attention.[7]
- CryptoCombiner is one of the most vetted actors on Exploit, having joined in April 2022 and has made 488 posts as of the writing of this report.



CryptoCombiner
Victoria Loves Care
Trusted
216
488 posts
Joined
04/12/22 (ID: 128791)
Activity
security / security
Deposit
13.548400 Ƀ

Posted 9 hours ago

For comrades who think that if you don't write about lockers and profit - this is dedicated to you
All topics containing:
- annual or monthly income of the company
- hospitals and hospitals
- administrative buildings (gas and water supply)
- schools and universities
- when you are looking for DA admin and pIntesters
This is a short list that makes it clear what not to do. There is no place for lockers in any of its manifestations on this forum. This is a kind of mugging. We are against it. All such topics will be banned along with the authors.

I will answer your questions in advance. We have not caved in to anyone. We do not want to be part of this movement. Such a way of earning money is highly questionable and is unacceptable for us. This will not happen on the forum. Period.

CryptoCombiner's Exploit post
Source: ZeroFox Intelligence

In the post, CyptoCombiner listed elements ***not*** to provide in advertisements on the forum, including:

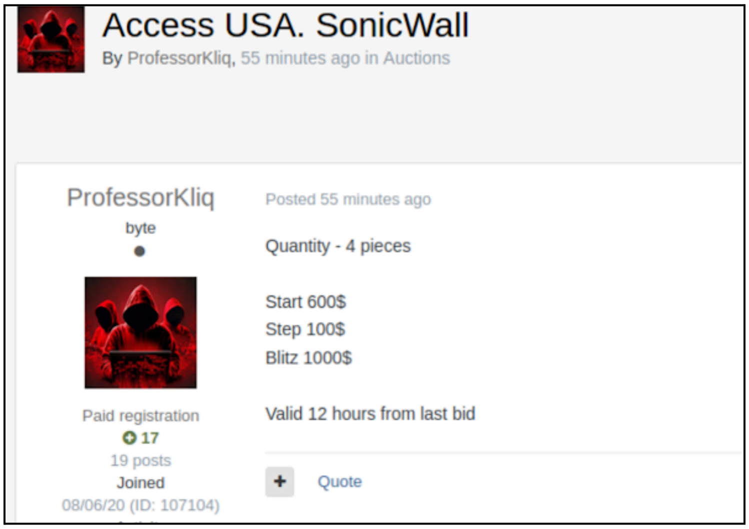
- Annual or monthly income of the company. This is one of the primary indicators used by security researchers and LE officials to identify the victim company, as these figures can sometimes be unique to a particular organization.
- Hospitals and medical facilities.
- Administrative buildings (such as gas and water supply companies).

[7] hXXps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa21-131a

- Schools and universities.
- Domain access admins and pentesters.

When advertising initial access to a victim organization, threat actors have historically provided details such as those listed above about the alleged victim company. This is almost certainly done to provoke interest from other potential threat actors; however, it also provides security researchers and officials with significant information that they can use to notify the victim organization.

- Notably, ZeroFox has observed that one of the most prominent initial access brokers on Exploit, "ProfessorKliq", has recently started posting offers without mentioning any specific details other than the type of access and the associated price. This demonstrates the type of behavior advised by CryptoCombiner and is likely to be emulated by other threat actors on the forum.



Access USA. SonicWall

By ProfessorKliq, 55 minutes ago in Auctions

ProfessorKliq
byte

Paid registration
17
19 posts
Joined
08/06/20 (ID: 107104)

Posted 55 minutes ago

Quantity - 4 pieces

Start 600$
Step 100$
Blitz 1000$

Valid 12 hours from last bid

An advertisement by ProfessorKliq on Exploit

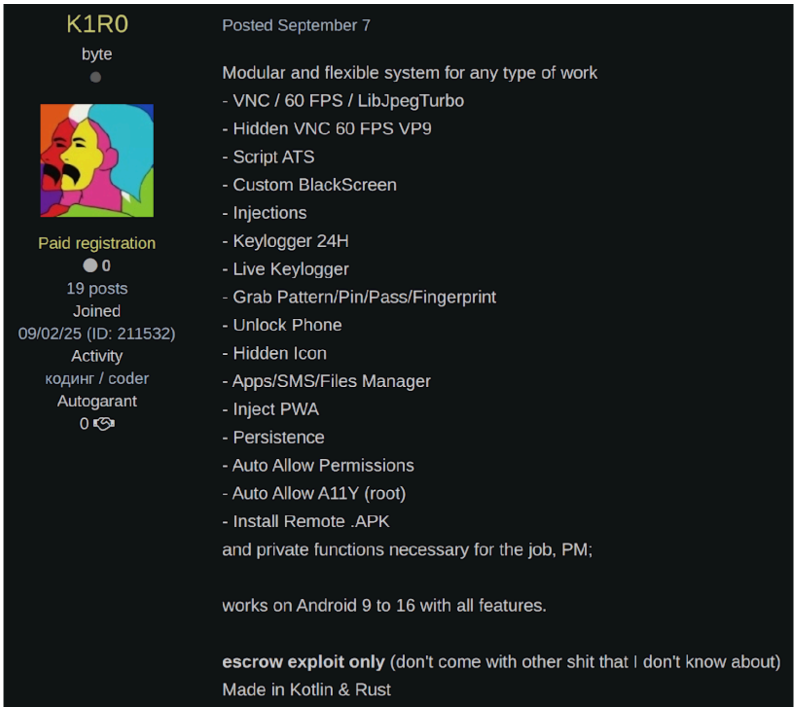
Source: ZeroFox Intelligence

A reduction in the amount of information that threat actors share about their targets will almost certainly make it more difficult for LE entities and security researchers to identify specific victims. One of the few remaining ways to identify a victim would be through direct communication with the seller, attempting to extract more details about the target. However, it is likely that this approach will cause sellers to be more cautious when dealing with potential buyers to further avoid detection.

New Android Botnet Advertised Dark Web Forum

On September 7, 2025, an actor using the alias “K1R0” posted on the dark web forum Exploit, advertising the sale of a new Android botnet called “Herodotus” for a monthly rental price of USD 4,000 (a test version is available for USD 700). K1R0 provided a list of specifications for the botnet, indicating Herodotus would enable users to:

- Discreetly surveil everything the target does
- Steal credentials, PINS, patterns, and messages
- Control the device remotely
- Hide and persist without detection
- Obtain a host of personally identifiable information (PII), which would almost certainly be used for social engineering campaigns in further malicious campaigns.



K1R0
byte

Paid registration
0
19 posts
Joined
09/02/25 (ID: 211532)
Activity
кодинг / coder
Autogarant
0

Posted September 7

Modular and flexible system for any type of work
- VNC / 60 FPS / LibJpegTurbo
- Hidden VNC 60 FPS VP9
- Script ATS
- Custom BlackScreen
- Injections
- Keylogger 24H
- Live Keylogger
- Grab Pattern/Pin/Pass/Fingerprint
- Unlock Phone
- Hidden Icon
- Apps/SMS/Files Manager
- Inject PWA
- Persistence
- Auto Allow Permissions
- Auto Allow A11Y (root)
- Install Remote .APK
and private functions necessary for the job, PM;

works on Android 9 to 16 with all features.

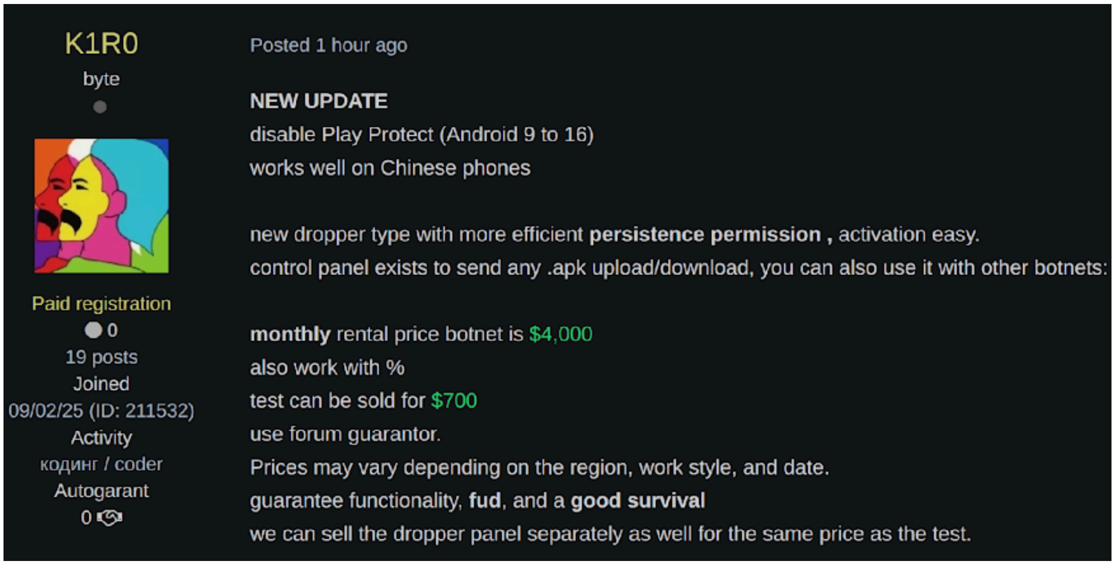
escrow exploit only (don't come with other shit that I don't know about)
Made in Kotlin & Rust

K1RO’s Exploit post

Source: ZeroFox Intelligence

Later, on September 16, 2025, K1R0 updated the thread, adding that Herodotus can disable Play Protect across Android versions and that it works well on Chinese phones as well. Further, K1R0 added that Herodotus can be used in conjunction with other botnets such as btmov/cracks, ermarc/hook, octo, hydra, tremendous, phoenix and teabot/ankras. The updated post with additional information was almost certainly an attempt to appeal to a wider target audience on the forum.

- K1R0 joined Exploit on September 2, 2025, and has not been verified as of writing but has expressed interest in offering escrow, likely to boost their credibility. They have provided extensive details regarding the features of the botnet and the pricing, likely to establish legitimacy about their claims and increase buyer interest in the product.



K1R0
byte

Paid registration
● 0
19 posts
Joined
09/02/25 (ID: 211532)
Activity
кодинг / coder
Autogarant
0

Posted 1 hour ago

NEW UPDATE
disable Play Protect (Android 9 to 16)
works well on Chinese phones

new dropper type with more efficient **persistence permission ,** activation easy.
control panel exists to send any .apk upload/download, you can also use it with other botnets:

monthly rental price botnet is $4,000
also work with %
test can be sold for $700
use forum guarantor.
Prices may vary depending on the region, work style, and date.
guarantee functionality, **fud**, and a **good survival**
we can sell the dropper panel separately as well for the same price as the test.

K1RO's updated Exploit post

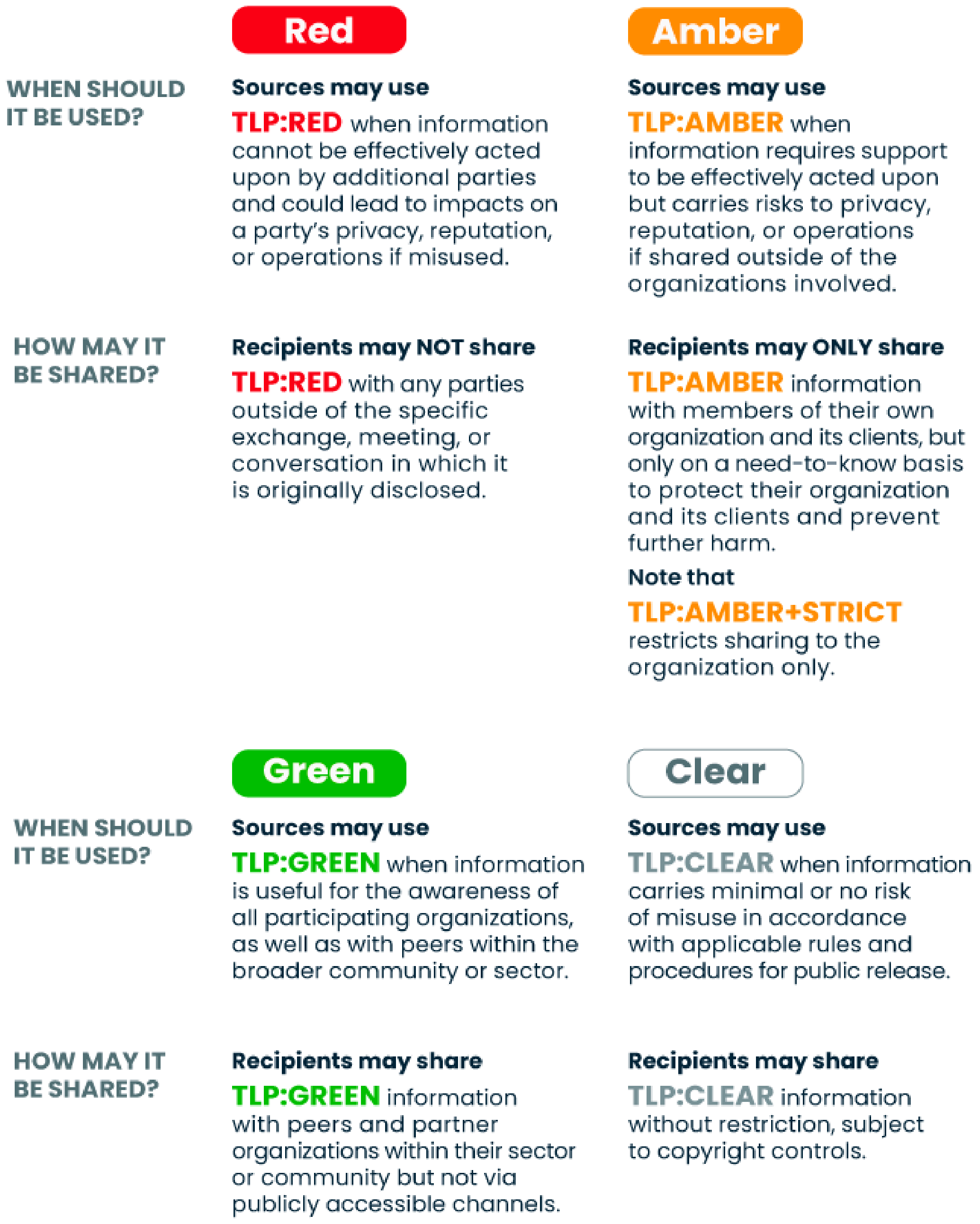
Source: ZeroFox Intelligence

Herodotus represents a sophisticated botnet that will likely generate significant interest from potential threat actors who are financially motivated or seeking to collect various PII in order to conduct a host of social engineering campaigns. Herodotus has likely been designed to allow even low-skilled attackers to use it, opening up a greater pool of threat actors. If legitimate, it is likely that Herodotus will cause significant financial damage against its targets and enable the exfiltration of sensitive data from mobile devices worldwide.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

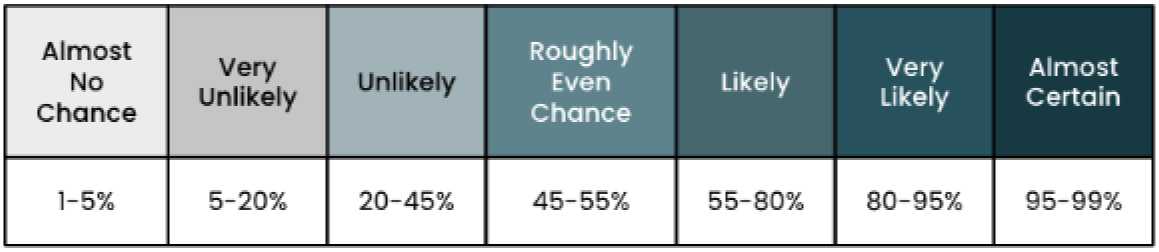


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%